UNIVERSIDAD POLITÉCNICA SALESIANA
SEDE QUITO

CARRERA: INGENIERÍA DE SISTEMAS

Tesis previa a la obtención del título de: INGENIERO DE SISTEMAS

TEMA:

PROPUESTA DE MONITOREO DE LA INFRAESTRUCTURA TECNOLÓGICA DE LOS SERVIDORES DEL MINISTERIO DE FINANZAS, BASADO EN EL MODELO ITIL V3 Y EN LA HERRAMIENTA HP SITESCOPE.

AUTOR:

WILMAN DARÍO SÁNCHEZ PICO

DIRECTOR:

ALBERTO RUSBEL DUCHI BASTIDAS

Quito, abril del 2014

DECLARATORIA DE RESPONSABILIDAD Y AUTORIZACIÓN DE USO DEL TRABAJO DE GRADO

Yo Wilman Darío Sánchez Pico autorizo a la Universidad Politécnica Salesiana la publicación total o parcial de este trabajo de grado y su reproducción sin fines de lucro.

Además declaro que los conceptos y análisis desarrollados y las conclusiones del presente trabajo son de exclusiva responsabilidad del autor.

WILMAN DARÍO SÁNCHEZ PICO
CC: 1720857984

DEDICATORIA

Dedico este trabajo a Dios, a mi familia, a mis padres, especialmente a mi madre por estar siempre a mi lado y brindarme su apoyo incondicional.

Wilman Sánchez

AGRADECIMIENTO

Agradezco a todas las personas que colaboraron con este trabajo, a los docentes de la Carrera de Sistemas, a mi tutor de tesis, al Ministerio de Finanzas y a la Universidad Politécnica Salesiana.

Wilman Sánchez

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

En el trabajo de titulación se realizaron actividades de monitoreo dirigidas a la infraestructura tecnológica actual de los servidores pertenecientes a los sistemas eSigef y eSipren, a cargo de la Dirección Nacional de Operaciones, haciendo uso de la herramienta HP SITESCOPE y siguiendo las recomendaciones enfocadas al marco de referencia ITIL V3. El propósito principal fue el realizar un proceso de monitoreo de manera ordenada y desarrollando un conjunto de procedimientos que ayudarán de cierta forma a lograr calidad y eficiencia en las operaciones de infraestructura. Como resultado de este proyecto se obtuvo el análisis de los principales equipos de infraestructura y la gestión de riesgo en la Dirección Nacional de Operaciones, lo que permitirá ofrecer un monitoreo proactivo ayudando a la toma de decisiones correctas y adecuadas que contribuirán a incentivar la investigación y adquisición de nuevas tecnologías para ofrecer un mejor servicio.

ABSTRACT

The monitoring work activities to the current technological infrastructure servers belonging to eSIGEF and eSipren systems, by the Dirección Nacional de Operaciones were performed, using HP SITESCOPE tool and following the recommendations focused on the framework ITIL V3. The main purpose was to conduct a monitoring process in an orderly manner and developing a set of procedures that will help in some way to achieve quality and efficiency in infrastructure operations. As a result of this project the analysis of the main infrastructure equipment and risk management in the Dirección Nacional de Operaciones was obtained, which will provide proactive monitoring to help making the right decisions and appropriate help to encourage research and acquisition of new technologies to provide better service.

INTRODUCCIÓN

El objetivo del trabajo es realizar una propuesta de monitoreo a la infraestructura tecnológica de los servidores del Ministerio de Finanzas, basado en el modelo ITIL V3 y haciendo uso de la herramienta HP SITESCOPE.

El documento se encuentra dividido en 4 capítulos, los cuales recogen las ideas en que se fundamenta el desarrollo del trabajo de titulación. En el capítulo 1, se realizó una introducción de las necesidades de la Dirección Nacional de Operaciones, además se plantea los objetivos, justificación y el alcance del proyecto.

En el capítulo 2, se da a conocer las ideas fundamentales, términos y definiciones que se utilizan en el desarrollo del proyecto para una mejor compresión del lector.

En el capítulo 3, se presenta el análisis de la Dirección Nacional de Operaciones, la documentación de los procesos referentes al monitoreo de la infraestructura tecnológica de los servidores donde se utiliza ITIL V3, y una introducción a la herramienta HP SITESCOPE que son parte del objetivo donde se realiza la explicación de las configuraciones de monitorización de los servidores establecidos en la misma.

En el capítulo 4, se incluye la propuesta de monitoreo con sus actividades correspondientes, los procedimientos de monitoreo de infraestructura tecnológica del centro de datos del Ministerio de Finanzas considerando las recomendaciones de ITIL V3, y se detallan los temas relacionados con la notificación de incidencias y problemas que se debe realizar.

Finalmente, se plantean las conclusiones y recomendaciones del proyecto.

CAPÍTULO 1
ANTECEDENTES

Descripción del proyecto

El trabajo de titulación "Propuesta de monitoreo de la infraestructura tecnológica de los servidores del Ministerio de Finanzas, basado en el modelo ITIL V3[1] y en la herramienta HP SITESCOPE", tiene como finalidad proponer procedimientos de monitoreo, para los servidores de infraestructura de los servicios eSigef y eSipren de la Dirección Nacional de Operaciones, considerando las recomendaciones de los procesos de Gestión de Disponibilidad y eventos de ITIL V3, que se apoyan en el monitoreo de infraestructura.

Planteamiento del problema

Es importante indicar que el Ministerio de Finanzas del Ecuador, es el ente rector de las Finanzas Públicas, reconocido como una entidad moderna orientada a brindar servicios públicos con calidad y oportunidad.

> La gestión de innovación de las finanzas públicas cuya misión es innovar de manera permanente los conceptos, metodologías, procesos, tecnologías y servicios inherentes al sistema nacional de las finanzas públicas, para contribuir a una mayor eficiencia y efectividad en la gestión de las finanzas públicas. La Dirección Nacional de Operaciones cuya misión es garantizar la operación, seguridad y disponibilidad de la infraestructura tecnológica que soportan las aplicaciones de software del Sistema Nacional de Finanzas Públicas, en cumplimiento a los acuerdos de niveles de servicio establecidos. (Ministerio de Finanzas, 2013).

Para la Dirección Nacional de Operaciones es importante realizar el monitoreo de la infraestructura tecnológica de los servicios eSigef y eSipren, con la finalidad de garantizar la disponibilidad y funcionamiento. Por este motivo, la estrategia a considerar es la generación de reportes de monitoreo de los servidores críticos a través de un

[1] V3: versión 3

proceso de monitoreo durante los 365 días del año y de ésta manera detectar incidentes y problemas ocurridos en la infraestructura tecnológica y resolverlos.
La propuesta de monitoreo, se apoya en los procesos de gestión de disponibilidad, nivel de servicio, continuidad, configuraciones, incidentes y problemas; que están apegados al marco de referencia ITIL V3 y en la herramienta de monitoreo HP SITESCOPE.

Justificación del proyecto

Una de las responsabilidades de la Dirección Nacional de Operaciones, es garantizar la disponibilidad de los principales sistemas de las Finanzas Públicas. Para realizar esta actividad se debe monitorear y controlar diariamente cada una de los recursos tecnológicos (procesador, memoria, disco y aplicaciones) de los servidores y aplicaciones de los sistemas.

En este proyecto se realizó un diagnóstico de la situación actual de la infraestructura tecnológica de los servidores del centro de datos del Ministerio de Finanzas, posterior se presenta la propuesta de monitoreo basada en ITIL V3.

Objetivos

1.4.1. Objetivo general.

- Realizar una propuesta de monitoreo para la infraestructura tecnológica de los servidores del Ministerio de Finanzas, que están a cargo de la Dirección Nacional de Operaciones, haciendo uso de la herramienta HP SITESCOPE y siguiendo las recomendaciones del modelo ITIL V3.

1.4.2. Objetivos específicos.

- Identificar y analizar los procesos de Gestión de Disponibilidad y Gestión de Eventos de ITIL V3, para que se ajusten a los requerimientos de monitoreo en la Dirección Nacional de Operaciones.
- Analizar la infraestructura tecnológica (servidores, software base) de los servicios eSigef y eSipren, para conocer las funciones (servidores web de presentación, aplicación, sistemas operativos, etc.), que se realizan.

- Efectuar el análisis de las funciones principales de la herramienta HP SITESCOPE y determinar sus beneficios para administración de monitorización de los servidores que actualmente están configurados.
- Realizar la propuesta de monitoreo para los servidores de infraestructura, basándose en los procesos de Gestión de Disponibilidad y eventos del modelo ITIL V3; con la finalidad de mejorar los procedimientos de monitoreo y definir responsables para la Gestión de Disponibilidad y Gestión de Eventos, a fin de mejorar un apropiado manejo de los recursos de infraestructura correspondientes a los servidores monitoreados.

Alcance del proyecto

El proyecto tiene como alcance el desarrollo y entrega a la Dirección Nacional de Operaciones de una propuesta de monitoreo en base a ITIL V3, teniendo como antecedentes la situación actual de la Dirección. Además esta propuesta está dirigida hacia la infraestructura tecnológica de servidores (hardware y software base), sin infraestructura de redes.

Un punto importante a considerar en la propuesta de monitoreo, es que la infraestructura tecnológica de los servidores está ubicada en el centro de datos principal (Quito). De esta manera el levantamiento de información se realizará de manera más rápida, a fin de realizar un proceso de monitoreo apoyado en la herramienta HP SITESCOPE la cual ayudará en el monitoreo.

CAPÍTULO 2
MARCO TEÓRICO

2.1. Itil V3

En este capítulo se definen los conceptos del conjunto de buenas prácticas ITIL V3, la definición de infraestructura tecnológica de servidores, evaluación de riesgos y la herramienta de monitoreo HP SITESCOPE. Según consultas realizadas en internet, tesis de ingeniería, documentos de procesos de la Dirección Nacional de Operaciones etc.

En la actualidad, la información que manejan las empresas es la fuente vital de sus actividades. Con los adelantos tecnológicos se busca realizar el procesamiento de la información en forma rápida y confiable lo que ha motivado a los servicios a acoplarse directamente con las necesidades y objetivos de la empresa.

Así también, el uso inadecuado, el no seguimiento y la falta de administración del área tecnológica expone a las empresas a:

- Incrementar de costos y horas improductivas
- Incumplimiento de los objetivos del negocio.

Es por esto, que en toda empresa debe existir un conjunto de prácticas para la gestión de servicios tecnológicos y un conjunto de procedimientos de gestión como por ejemplo el conjunto de buenas prácticas ITIL.

> El estándar ITIL, es un conjunto de directrices de buenas prácticas para alinear los recursos humanos, los procesos y la tecnología a la necesidad de optimizar la eficacia de la gestión de servicios. Fue desarrollado al reconocer que las organizaciones dependen cada vez más de la informática, esto conduce a la necesidad de organizar servicios de calidad que logren satisfacer los requerimientos del negocio, como las necesidades que se originan de los usuarios. (Osiatis, 2011)

Statum, una empresa dedicada al nexo entre tecnología y negocio, establece que no es una doctrina ni de un modelo rígido, si bien ITIL proporciona directrices sobre buenas

prácticas, su implementación difiere según la realidad de cada organización. (STATUM, 2014).

ITIL reunió a las empresas más exitosas para extraer las mejores prácticas de trabajo alcanzadas mediante el uso de esta herramienta, las características más resaltadas fueron:

- Aplicación de código abierto, de uso público, sin anclaje al fabricante.
- Fácil de aplicar en todo tipo de empresa.
- Evolución permanente gracias a la contribución de la comunidad ITIL. (Osiatis, 2011).

2.2. Generalidades de ITIL V3

ITIL fue publicado entre 1989 y 1995, por la oficina de publicaciones del gobierno Británico motivado por la agencia central de comunicaciones y telecomunicaciones. En el año 2007 ITIL V2 fue sustituida por una mejorada y consolidada tercera versión, la misma que consiste en 5 libros que cubren el ciclo de vida completo del servicio. (Bon, 2008, p. 28)

A continuación se presenta un mapa con la evolución de ITIL:

Figura 1 Evolución de ITIL

Fuente: Osiatis ITIL V3, 2011

Los cinco libros de ITIL V3, cubren cada etapa del ciclo de vida del servicio.

2.3. Etapas del ciclo de vida del servicio

2.3.1. Ciclo de vida de los servicios.

> ITIL V 3, estructura la gestión de los servicios de tecnologías de información sobre el concepto de ciclo de vida de los servicios. Este enfoque tiene como objetivo ofrecer una visión global de la vida de un servicio desde su diseño hasta su eventual abandono, sin por ello ignorar los detalles de todos los procesos y funciones involucrados en la eficiente prestación del mismo. El ciclo de vida del servicio, consta de cinco fases que se corresponden con los nuevos libros de ITIL. (Osiatis, 2011).

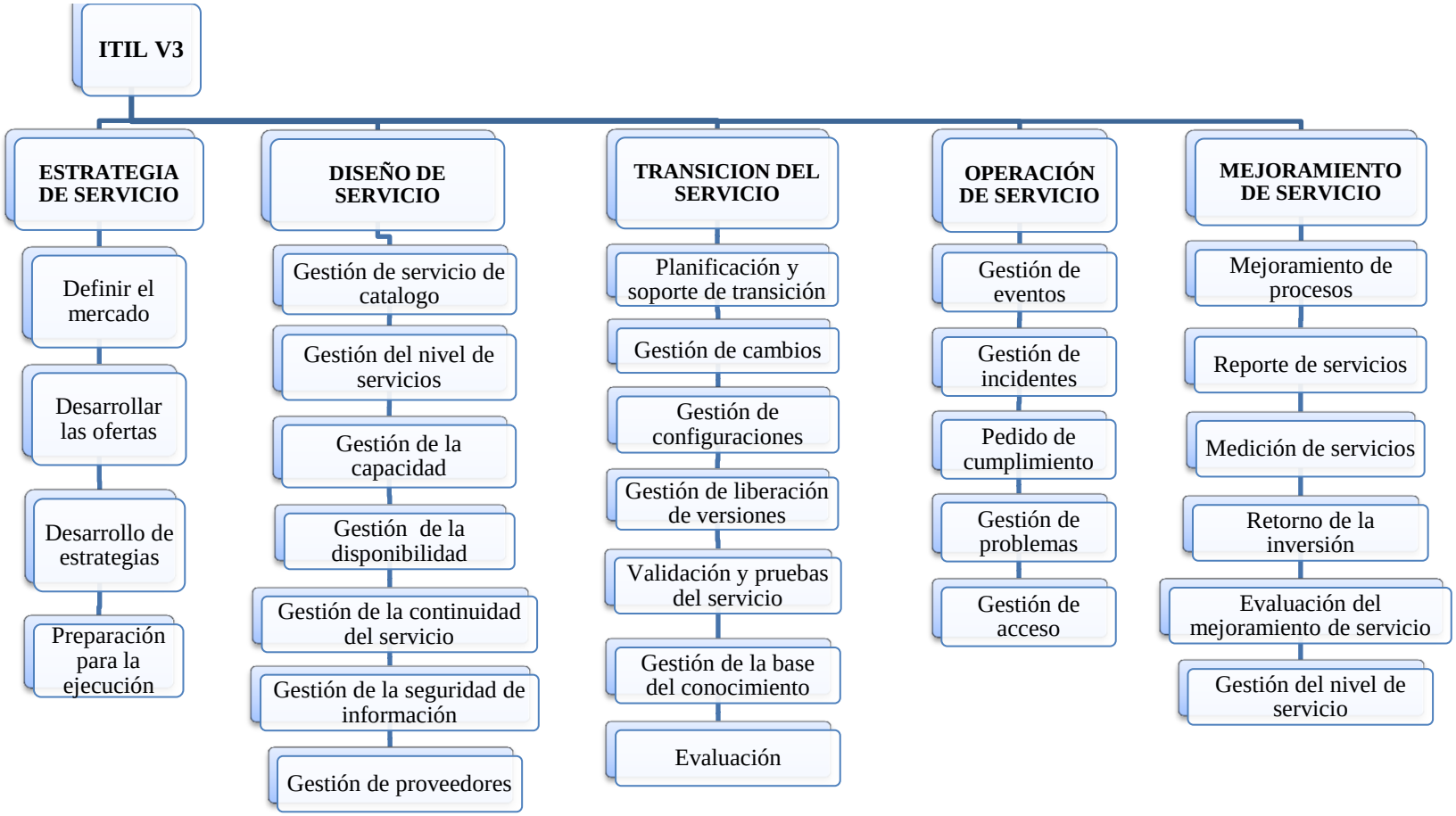
Cabe indicar que estas fases cumplen un ciclo de vida cíclico, debido a que ITIL recomienda que la gestión de servicios se mantenga en un periodo de mejora continua y para eso siempre se deberá mantener cumpliendo el orden en el que se encuentran estas fases, como están descritas a continuación:

1. Estrategia del Servicio
2. Diseño del Servicio
3. Transición del Servicio
4. Operación del Servicio
5. Mejora Continua del Servicio

2.4. Estructura de ITIL V3

En el siguiente diagrama se muestran las fases del ciclo de vida de ITIL V3, con sus procesos y funciones:

Figura 2 Estructura de ITIL



Fuente: Van Haren Publishing, 2008, pág. 111

En proyecto de titulación, se tomará en cuenta los procesos de Gestión de Disponibilidad y de eventos de las fases que están descritas en la figura 2; relacionadas con el marco de referencia ITIL V3. Debido a que estos dos procesos son clave para el monitoreo, por lo tanto son de mucha ayuda, al momento de vincular el monitoreo de infraestructura tecnológica de los servidores del Ministerio de Finanzas, con las mejores prácticas de ITIL V 3.

Además para apoyo de la Gestión de Disponibilidad y de eventos, también se describen brevemente algunos procesos relacionados con la disponibilidad y el monitoreo de infraestructura en la tabla 1.

Tabla 1

Fases y procesos de ITIL

Fases	Procesos
Diseño	Niveles de Servicio Gestión de Disponibilidad Gestión de la Continuidad
Transición	Gestión de Configuraciones
Operación	Gestión de Eventos Gestión de Incidencias Gestión de Problemas

Elaborado por: Wilman Sánchez

2.4.1. Fase Diseño del Servicio.

"Provee guías para el diseño y el desarrollo de servicios, así como procesos para la gestión de servicios." (Long, 2012, p. 5-24). El Diseño del Servicio no está limitado a la creación de nuevos servicios, asimismo se incluyen las mejoras y cambios necesarios para incrementar el nivel de servicio a los clientes durante todo el ciclo de vida. El principal objetivo de esta fase es diseñar nuevos servicios o modificar los existentes, para incorporar al catálogo de servicios y posteriormente al entorno de producción.

2.4.1.1. Gestión de Nivel de Servicio.

La Gestión de Nivel de Servicio (SLM) es esencial en una organización, de tal forma que el nivel se servicios de tecnologías de información que se necesita para soportar una compañía, pueda ser determinado y monitorizado identificando

si los niveles de servicio requeridos se están llevando a cabo, y en caso de que no se estén llevando acabo, por qué no. (Bon, 2008, p. 28)

Según Bon, uno de los principales propósitos de este proceso, es poner la tecnología al servicio del cliente, para ello se realizan negociaciones, acuerdos y la documentación formal que reflejen el nivel de servicio que efectúen con los objetivos del negocio, a partir de esta referencia se debe cumplir el monitoreo y la generación de reportes del nivel de servicio suministrado.

2.4.1.2. Gestión de la Disponibilidad.

Los procesos de Gestión de Disponibilidad, se utilizan para optimizar la capacidad de la Infraestructura tecnológica, los servicios y la organización de soporte para entregar un coste efectivo y un sostenido nivel de disponibilidad, que asegura a la empresa la satisfacción de sus objetivos empresariales. (Bon, 2008, p. 28)

Esto se logra mediante la determinación de requerimientos de disponibilidad de la empresa y la unión a la capacidad de la infraestructura y la organización de soporte. En el lugar donde no calzan los requerimientos y las capacidades, la Gestión de Disponibilidad asegura que la empresa sea proveída con alternativas disponibles y asociadas a las opciones de costes.

El objetivo de este proceso es afirmar que el nivel de servicio con respecto a la disponibilidad esté transmitido de acuerdo a las necesidades del negocio, tomando en cuenta el costo frente al beneficio. Optimizando y monitorizando los servicios de tecnologías de información; para que funcionen ininterrumpidamente y de manera fiable, cumpliendo los SLAs[2] y todo ello a un coste razonable.

2.4.1.3. Gestión de la Continuidad.

Son todas las actividades que involucran mantener operativos los servicios de TI en la empresa. Se preocupa de impedir una imprevista y peligrosa interrupción de los servicios, debido a desastres naturales u otras fuerzas de causa mayor, tenga consecuencias catastróficas para el negocio.

[2] Niveles de servicio establecidos

Para esto se trabaja en cada fase del ciclo de vida de los servicios, con procedimientos de recuperación que deben estar alineados con el plan de continuidad de la empresa.

2.4.2. Fase Transición del Servicio.

La transición del servicio permite identificar los productos y servicios definidos en la fase de Diseño del Servicio, para que se integren en el entorno de producción y sean accesibles a los clientes y usuarios autorizados. (Long, 2012, p. 5-24). Esto muestra como los requerimientos de estrategia de servicio que están codificados en el diseño de servicio y son correctamente implementados en la operación de servicio.

2.4.2.1. Gestión de Configuraciones.

Provee soporte al negocio mediante la emisión de información actualizada y correcta sobre toda la infraestructura tecnológica de la empresa.

2.4.3. Fase de Operación.

Esta fase pretende dar efectividad y eficiencia en el suministro y soporte de servicios, tomando en cuenta las necesidades de los clientes. (Long, 2012, p. 5-24) Los aspectos esenciales en la fase de Operación del Servicio es la búsqueda de un equilibrio entre estabilidad y capacidad de respuesta.

2.4.3.1. Gestión de Eventos.

"La Gestión de Eventos es el proceso responsable de gestionar eventos a través de su ciclo de vida, que incluyen ocurrencia, detección, filtro, lanzar alguna acción si fuera necesaria, revisión y cierre." (Osiatis, 2011).

Según el sitio web de Osiatis, entre otras, las actividades que se realizan son: aparición de eventos, notificación de eventos, detección y filtrado de eventos, clasificación de eventos, correlación, disparadores, opciones de respuesta y la revisión de acciones y cierres; todo esto como un proceso sistémico.

2.4.3.2. Gestión de Incidentes.

Tiene como objetivo satisfacer de la forma más rápida y eficaz posible, cualquier incidente que cause una interrupción en el servicio. En ITIL el incidente se especifica como la interrupción o pérdida de la calidad de TI que no está contemplada en la planificación.

Dentro de la Gestión de Incidentes se incluyen fallas o consultas que formulan los usuarios de la aplicación desde el interior de la empresa, ya sea por vía telefónica o de escritorio. También pueden ser fruto del resultado de la administración al efectuar el monitoreo de rutina.

2.4.3.3. Gestión de Problemas.

ITIL, define un problema como la causa de uno o más incidentes. (Bon, 2008, p. 28). La Gestión de Problemas puede ser:

- **Reactiva**: Analiza los incidentes ocurridos para descubrir su causa y entiende soluciones a los mismos.
- **Proactiva**: Monitoriza la calidad de la infraestructura TI y analiza su configuración con el objetivo de prevenir incidentes incluso antes de que éstos ocurran.

2.5. Descripción de los servicios a ser monitoreados

2.5.1. Servicio.

Un servicio es, un medio para otorgar valor a los clientes facilitándoles un resultado deseado sin la necesidad de que estos asuman los costes y riesgos específicos asociados. (Osiatis, 2011).

2.5.2. Sistema eSigef.

> "El sistema de administración financiera del sector público (eSigef), utiliza para su operación y seguridad un esquema de funciones y usuarios que determinan

permisos sobre los objetos de la aplicación. De esta manera se habilitan o restringen ciertas operaciones a los usuarios". (Ministerio de Finanzas, 2013).

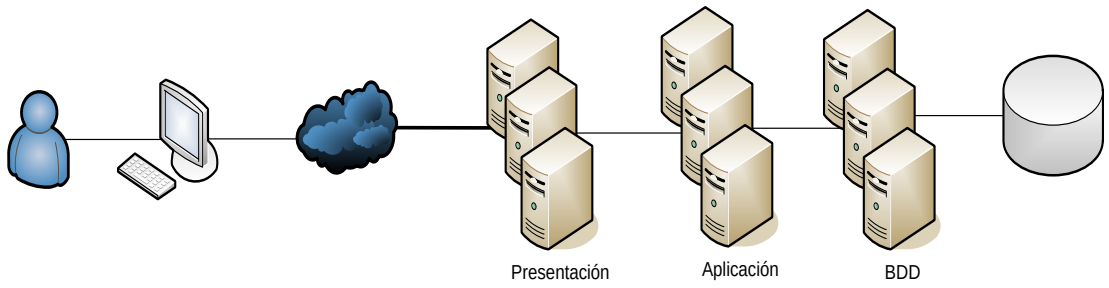
El modelo de administración de usuarios y permisos determina que las personas para realizar cualquier operación en el sistema, requieran de autorizaciones que se encuentran definidos en los perfiles asociados a las funciones, los que a su vez se relacionan con los usuarios para determinar el nivel de acceso a la aplicación. (Ministerio de Finanzas, 2013).

2.5.2.1 Infraestructura tecnológica de los servidores de eSigef.

La infraestructura tecnológica de eSigef, está conformada por:

- Servidores de la capa de presentación.
- Servidores de la capa de aplicación
- Servidores de la capa de base de datos.

Figura 3 Estructura del sistema eSigef



Fuente: Otorgada por el Ministerio de Finanzas, 2014

2.5.3. Sistema eSipren.[3]

Para el pago de nómina, se ha implementado un control (eSipren), que permite validar la existencia del servidor público en el distributivo de remuneraciones, sueldos y salarios básicos aprobado por el Ministerio de Finanzas para cada ejercicio fiscal. El sistema eSipren, permite consolidar y validar cada orden de

[3] Sistema Presupuestario de Remuneraciones y Nómina

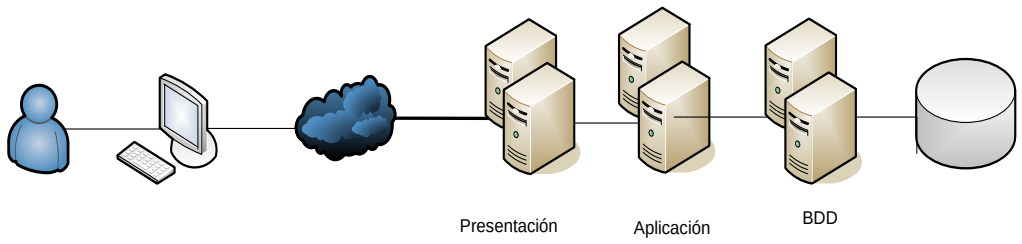
nómina, para luego aprobarla y generar el CUR[4] de compromiso y devengado con el correspondiente asiento contable para proceder al pago y finalmente ejecutarla transferencia al Banco Central del Ecuador. (scribd, 2011).

2.5.3.1. Infraestructura tecnológica de los servidores de eSipren.

La infraestructura tecnológica de eSipren, está conformada por:

- Servidores de la capa de presentación.
- Servidores de la capa de aplicación.
- Servidores de la capa de base de datos.

Figura 4 Estructura del sistema eSipren



Fuente: Otorgado por el Ministerio de Finanzas

2.6. Herramientas de monitoreo

En esta sección se realiza una breve descripción de algunas herramientas de monitoreo, de software libre y comerciales; más populares y utilizadas en la actualidad. Con el objetivo de ser comparadas con la herramienta HP SITESCOPE, que sirve de apoyo para la realización de trabajo del trabajo de titulación.

Para describir de mejor manera las herramientas de monitoreo se realiza la diferencia entre herramientas de software libre y las herramientas comerciales, describiendo las ventajas e inconvenientes de cada una de ellas.

[4] Cuenta Única de Retenciones

2.6.1. Herramientas de software libre.

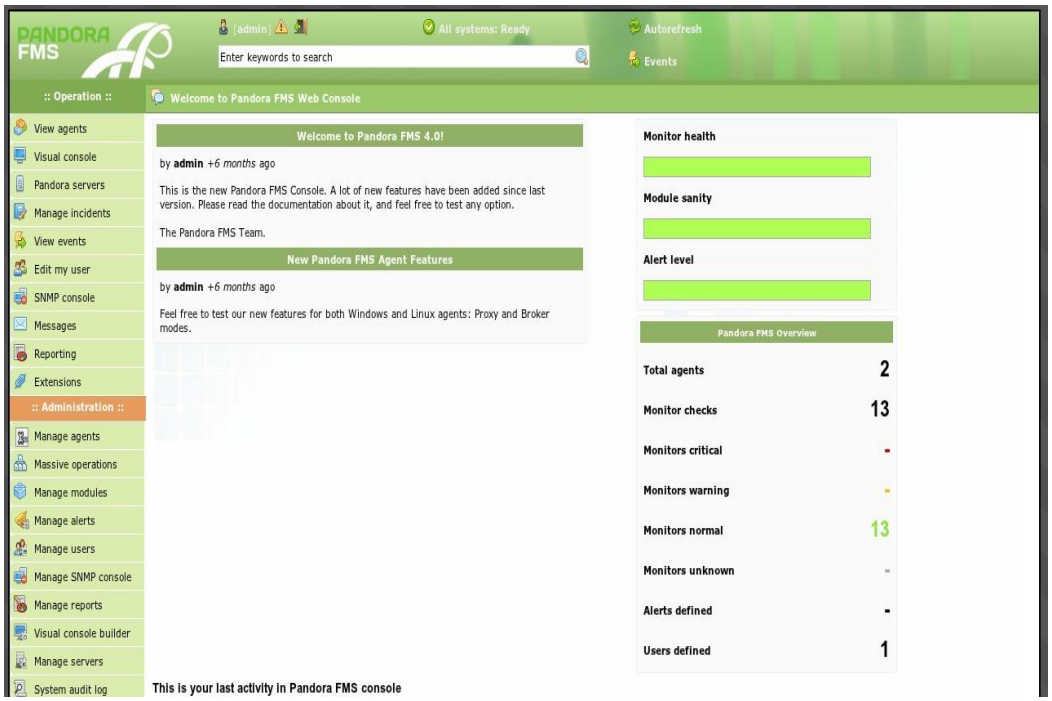
Son herramientas de distribución libre. Su principal ventaja es el bajo costo de adquisición y la innovación, corrección de errores por parte de cualquier usuario. De este tipo de herramientas, se describen las siguientes:

- Pandora FMS
- Nagios

Pandora FMS: Es una herramienta con licencia GPL[5] la cual está orientada a proteger la libre distribución y modificación de software libre. La publicación de la primera versión de esta herramienta empezó en el año 2004, con el nombre de "Pandoramon". Actualmente está desarrollado y mantenido por la empresa Ártica con base en Madrid. Existe una versión con una licencia comercial, llamada Pandora FMS Enterprise que proporciona numerosas características, aunque el 90% del código es similar a la versión OpenSource y se puede obtener por un precio proporcional al número de agentes o nodos instalados. (FMS, 2014). Esta herramienta trabaja con una base de datos **MySQL** que el único formato soportado, donde se almacena todos los datos recibidos por los módulos de los agentes, por lo tanto es el componente más vital de esta herramienta.

[5] GPL: Licencia Pública General de GNU

Figura 5 Interfaz o consola web de usuario de Pandora FMS



Fuente: pandorafms.org

Además, posee como entorno de usuario una consola web que permite la administración y control total de la herramienta, con diferentes privilegios según el usuario configurado (ver figura 5). Está programada en PHP[6] y no requiere la instalación de ningún software adicional: ni Java, ni ActiveX. Las gráficas están disponibles en FLASH y para poder verlas en este formato será necesario este complemento para el navegador. (FMS, 2014).

Ventajas:

- Esta herramienta cumple con todas las características de un sistema de monitorización, incluyendo la supervisión en todo tipo de sistemas operativos mixtos.
- La interfaz o consola web de Pandora FMS es de fácil uso, debido a que permite controlar completamente la aplicación de forma amigable, también realizar tareas de administración y configuración. También es de sencilla instalación y

[6] PHP: lenguaje de código abierto, adecuado para el desarrollo web

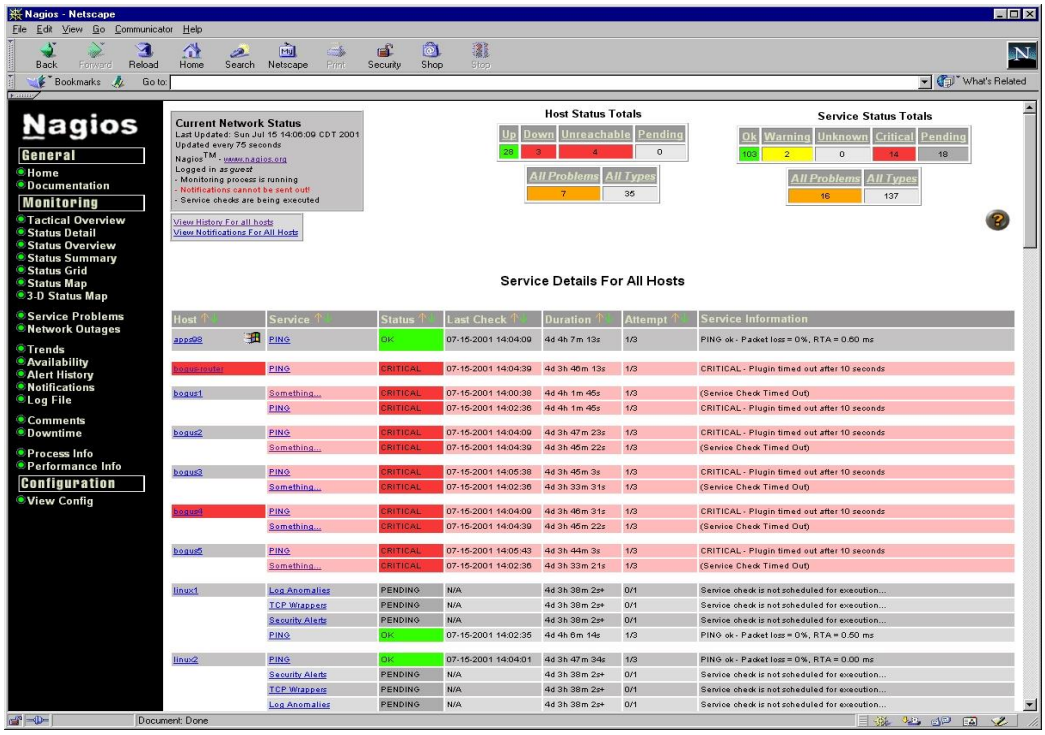
configuración debido a que el tiempo que conlleva es menor que la de otros sistemas, lo cual realza la facilidad de uso de cara al usuario.

- En cuanto a la arquitectura de esta herramienta, debido a ser un proyecto iniciado hace menos tiempo, se puede decir que su forma de avanzar hacia su objetivo es distinta y camina con mejor perspectiva hacia el funcionamiento y la consolidación de la herramienta, evitando errores que ya poseen otros sistemas de monitorización.

Nagios Core: Software libre orientado a la monitorización es hace varios años, Nagios Core es una herramienta Open Source, está diseñado y mantenido por el autor Ethan Galstad. En cuanto a la arquitectura de la herramienta, es un sistema de monitorización monolítico y orientado a eventos que vigila a equipos, tanto el hardware como software, alertando cuando el comportamiento de los mismos no es el adecuado. Puede monitorizar servicios de red, recursos hosts y puede programar plugins específicos para nuevos sistemas, el control remoto es manejado a través de túneles SSH o SSL cifrado. (Enterprices, 2009)

La interfaz web de esta herramienta visualiza a los servidores y el estado de los mismos. Además se puede organizar las máquinas o esclavos monitorizados si se realiza la configuración oportuna, en grupos de servicios.

Figura 6 Interfaz Web de Nagios



Fuente: es.wikipedia.org

Ventajas:

- Es un software muy conocido, debido a que posee una gran cantidad de complementos, para extender sus funcionalidades a través de innumerables sitios webs, que incluso son facilitados en su manual oficial.
- La fama de esta herramienta, ha incentivado a la creación de nuevas herramientas de monitorización que contienen un núcleo basado en Nagios, por ejemplo: Opsview o Shinkem.
- Existe amplia documentación muy elaborada, incluso detallada y facilitada por la comunidad de Nagios. (Nagios, 2012).

Inconvenientes:

- La instalación, configuración y los complementos es basada en texto, lo cual implica una dificultad media, inversión de tiempo y requiere un grado de conocimiento técnico para su correspondiente configuración. Cuando en realidad, la mayoría de estas funciones, alrededor del 90% ya son posibles a partir del protocolo SNMP.

- Si es necesario alguna modificación en la configuración de la herramienta, se requiere un reinicio completo del sistema, debido a que no es capaz de auto-descubrir nodos nuevos que se incluyan al sistema.
- La interfaz web sólo sirve para visualizar los acontecimientos, los cambios realizados deben revisarse manualmente desde el servidor de Nagios.
- Esta herramienta, no soporta ningún gestor de base de datos que trabaje bajo SQL. (Nagios.org, 2012).

2.6.2. Herramientas de software comercial.

> Estas herramientas son conocidas como software propietario o privativo y donde el usuario tiene limitaciones el uso, modificación y redistribución. La persona o compañía que posee los derechos de autor restringe los derechos de usuario y utiliza como fuente de productividad constituyendo un acuerdo o contrato con el cliente. (Lacoctelera, 2012).

De este tipo de herramientas, se analizarán las siguientes:

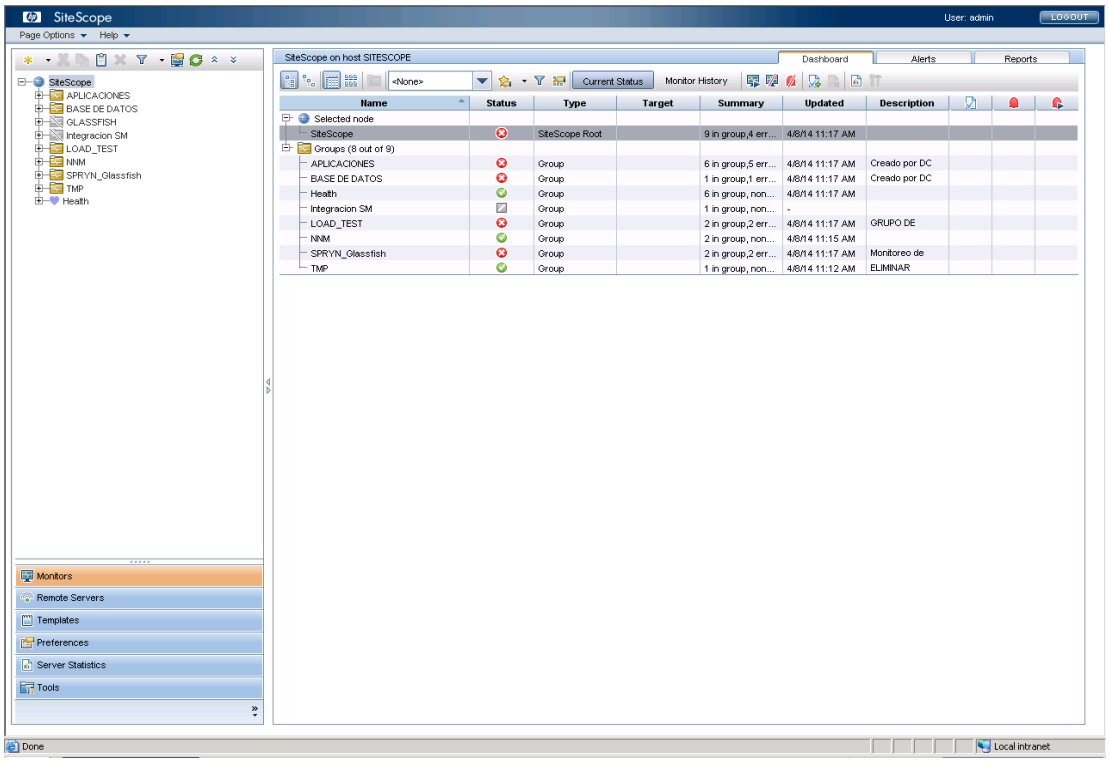
- HP SITESCOPE
- BMC Patrol

HP SITESCOPE: El software HP SITESCOPE, es una solución de supervisión sin agente diseñada para monitorizar la disponibilidad y rendimiento de las infraestructuras de servidores, sistemas operativos, dispositivos de red, servicios de red, aplicaciones. El monitoreo de infraestructura que realiza HP SITESCOPE, está basada en web que es un método ligero, altamente personalizable, no requiere de agentes para la colección de datos y se puede instalar en sistemas de producción. (Hewlett-Packard, 2012).

Además cuenta con más de 90 tipos de monitores que pueden supervisar la utilización, disponibilidad, uso de recursos; y una variedad de tipos de plataformas de aplicaciones. Puede ser configurado para alertar siempre que detecta un problema en la infraestructura, existen varios tipos de alertas, como el envío de mensajes por correo

electrónico, el envío de SNMP[7], o la ejecución de un script. También se puede crear informes para uno o varios monitores, incluso para varios grupos de monitores. Los informes muestran información acerca de cómo los servidores y las aplicaciones que se están supervisando, se han comportado a través del tiempo.

Figura 7 Entorno de HP SITESCOPE



Fuente: Otorgado por la Dirección de Operaciones

La herramienta además ofrece diferentes plantillas, que permiten desarrollar un conjunto estandarizado de tipos de monitores y configuraciones; en una única estructura. Estas plantillas pueden desplegarse con rapidez en toda la infraestructura para asegurarse que el monitoreo cumpla con las normas establecidas en la plantilla. También incluye tipos de alertas que se pueden utilizar para comunicar y registrar la información de eventos en una variedad de medios de comunicación (mensajes de texto, mails, scripts, logs). (Hewlett-Packard, 2012).

[7] SNMP: Protocolo simple de administración de red

Ventajas:

- Período de monitoreo rápido y efectivo para la infraestructura de TI y la supervisión de las aplicaciones en infraestructuras físicas, virtuales y en la nube.
- Supervisión inmediata para más de 100 aplicaciones diferentes.
- Plantillas de soluciones que incluyen las mejores prácticas recomendadas.
- Implementación rápida sin instalación de agentes; perfecta para los entornos en nube privada o híbrida.
- Previene que los ingresos de una compañía se vean afectados por las fallas de IT ya que proporciona respuestas proactivas antes de que ocurra un incidente.
- Ayuda a maximizar la disponibilidad de la infraestructura de IT y el monitoreo de más de 100 aplicaciones distintas.

Inconvenientes:

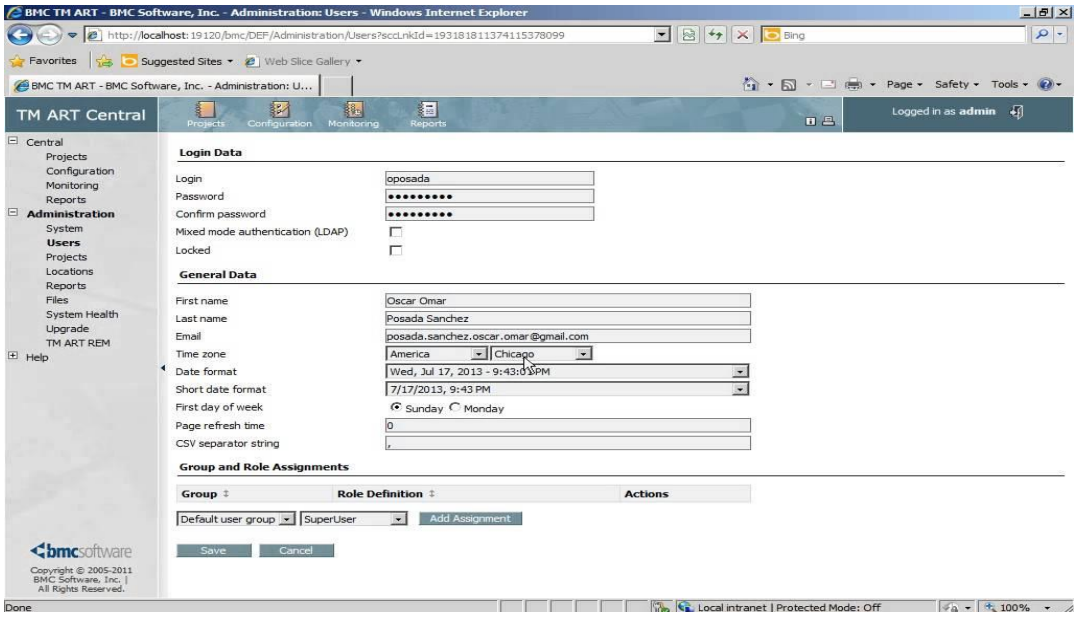
- No es un producto de software libre, este inconveniente presenta la desventaja del costo que las empresas tienen que adquirir por la licencia, a esto se le debe sumar un coste extra por cada agente que se desee instalar.

BMC Patrol: Esta herramienta fue creada en un principio para la gestión de sistemas y bases de datos que controlaba el estado de los equipos, recursos y aplicaciones en una red. Dicho software fue una adquisición de la empresa BMC, entre otras muchas pequeñas y medianas empresas, en concreto a Patrol Software, Inc de Australia. Actualmente, BMC Patrol se encuentra integrada como una parte del actual producto o software propio de IBM, la cual se define como una herramienta para la gestión distribuida de infraestructura y aplicaciones para garantizar un rendimiento óptimo. Esta solución intenta integrar en una única herramienta BMC Patrol clásico y BMC Patrol Express, cuya principal diferencia es el uso de una arquitectura con y sin agentes respectivamente. (BCM, 2014)

Presenta una interfaz de usuario denominada "BMC Performance Manager Portal" centralizada a través de un explorador web que permite gestionar el estado de una aplicación, sistema operativo, software intermediario o hardware. Posee paneles o vistas

personalizadas, gráficos, avisos y estados de eventos, además de un inicio de sesión por usuario; como muestra en la figura 8. (BMCsoftware, 2014).

Figura 8 Consola BMC Performance



Fuente: http://support.sas.com/rnd/emi/BMCPatrol/index.html

Ventajas:

- Es la mejor herramienta para gestionar una infraestructura de tecnologías de información, si se combina con algunas herramientas especializadas en la gestión en alguno de los campos citados como la infraestructura, bases de datos.

Inconvenientes:

- No es un producto de software libre y presenta un precio elevado por su licencia, además por cada agente a realizar el monitoreo respectivo.

2.6.3. Comparación entre herramientas.

Después de describir brevemente algunas de las herramientas de monitorización más populares y reconocidas, se compara entre todas las soluciones descritas, en base a los factores globales y competencias contenidas en dichos factores, los cuales se describen a continuación.

Funcionalidad:

- Monitorizar servicios, hardware y sistema operativo.
- Multiplataforma en cliente.
- Generar gráficas, informes y estadísticas.
- Enviar alarmas y notificaciones, etc.

Fácil uso:

- Interfaz o consola web con control total sobre la aplicación.
- Personalización de dicha interfaz.
- Extensión del sistema (plugins).
- Instalación, configuración y puesta en marcha.

Arquitectura:

- Basada en varios procesos que realicen las funcionalidades de la aplicación.
- Consumo y requisitos previos aceptables (hardware y software)
- Sistema con agentes que trabajan en cada cliente o nodo.
- Posibilidad de monitorizar gran cantidad número de nodos.

Soporte técnico:

- Desarrollo de nuevas mejoras y revisiones en la aplicación para la corrección de bugs.
- Actividad en el foro y wiki ante preguntas y resolución de problemas o peticiones de usuarios.

Tabla 2

Comparativa gráfica de las principales características de los sistemas de monitorización

Herramienta de monitoreo	Software libre	Funcionalidad	Fácil uso	Arquitectura	Soporte
Pandora FMS					
Nagios					

Herramienta de monitoreo	Software libre	Funcionalidad	Fácil uso	Arquitectura	Soporte
HP SITESCOPE	✗	✓	✓	✓	✓
BMC Patrol	✗	✓	✓	✓	✓

Elaborado por: Wilman Sánchez

Nota: ✓ La herramienta cumple con todas las competencias de ese factor.

✗ La herramienta NO cumple con al menos una de las competencias de ese factor.

Conclusión:

Después de realizar la comparación respectiva entre las herramientas de monitoreo, se concluye que existen dos herramientas que cumplen con todos los factores para realizar el monitoreo en la Dirección Nacional de Operaciones. La primera herramienta es "Pandora", por cumplir con todas las especificaciones de una completa herramienta de monitoreo. La segunda herramienta es HP SITESCOPE que actualmente forma parte de la infraestructura del centro de datos, cumple con la mayor parte de las especificaciones de la tabla 2 y cuenta con la ventaja de estar instalada en la Dirección Nacional de Operaciones desde el año 2012, razón por la cual se la elegirá como herramienta de monitoreo en el desarrollo de esta investigación.

2.7. Monitoreo de infraestructura tecnológica de los servidores

2.7.1. Introducción.

Un servicio proactivo para el control del estado de su infraestructura en tiempo real, es la mejor forma de propiciar una verdadera disponibilidad de los sistemas de tecnologías de información. Para asegurar y controlar el estado y la disponibilidad de la infraestructura de IT, se requiere un centro de operaciones que continuamente ejerza lo siguiente: (Cloud, 2010)

- **Detectar:** eventos críticos de la infraestructura de IT.
- **Analizar:** los requerimientos para su atención.
- **Coordinar:** las operaciones para la atención.
- **Informar:** a los proveedores de soporte para que se ejecuten las acciones.

Para solventar las necesidades anteriores, se debe invertir tiempo y recursos en:

- Automatización de las actividades de monitoreo.
- Soporte continuo a las herramientas de monitoreo.
- Instauración de procesos de Gestión de Eventos.
- Recursos disponibles las 24 horas por los 7 días de la semana, para la gestión del monitoreo y la coordinación de la atención de eventos.

2.7.2. Beneficios.

Dentro de los principales beneficios del monitoreo de la infraestructura están:

- Automatización de las actividades de monitoreo a través de herramientas que provean información en tiempo real del rendimiento, salud y estado de los activos informáticos.
- Atención y seguimiento de eventos al ser un punto de contacto con los proveedores de soporte del cliente, facilitando así el cumplimiento de los niveles de servicio.
- Entrega de reportes e informes que permiten el análisis histórico de la utilización y disponibilidad de sus activos informáticos.
- Se pueden detectar errores y consecuentemente generar mejoras a los servicios
- Establecer mediciones cuantitativas del uso de los servicios y recursos, para sustentar un crecimiento de las tecnologías de información.
- Con la generación de reportes del estado de los servicios, se puede asesorar en la toma de decisiones al negocio. (Cloud, 2010).

2.8. Evaluación de riesgos

Son actividades que determinan el nivel de exposición de un proceso frente a sus riesgos, esto con el propósito de desarrollar estrategias de mitigación, a través de la instauración y fortalecimiento de controles. Los conflictos pueden ser operacionales, estratégicos, de reporte, regulatorios o cumplimiento y de gobierno. (Deloitte, 2012).

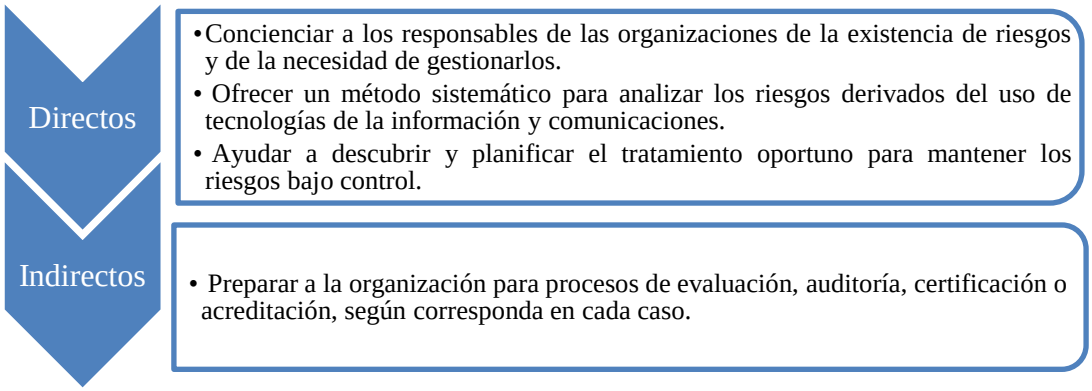
2.8.1. Magerit.

Es una metodología de análisis y gestión de riesgos orientada a los sistemas de información elaborada por el Consejo Superior de Administración Electrónica, para minimizar los riesgos en el uso de tecnologías de información[8].

Esta metodología está relacionada con las personas que trabajan con información digital y sistemas informáticos, para que la información o los servicios que sean valiosos, se puedan identificar los riesgos existentes y de esta manera ayudar a protegerlos. Conocer el riesgo al que están sometidos los elementos de trabajo y de esta manera permitirá ser gestionados. (MHAP, 2012)

Los objetivos que persigue Magerit, se puede observar en la figura 8.

Figura 9 Objetivos de Magerit



Fuente: (MHAP, 2012)

2.8.2. Fundamentos de gestión de riesgos.

En este apartado se realiza una breve descripción en lo que se refiere a la gestión de riesgos, con el objetivo de que este factor sirva de apoyo para la evaluación de riesgos que se desarrollará en el capítulo 3 del trabajo de titulación.

[8] MAGERIT: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información

2.8.2.1. Riesgo.

Es la exposición potencial a situaciones que afectan el logro de los objetivos de una organización, generando pérdidas. Se mide en requisitos de consecuencias y probabilidad. (Deloitte, 2012)

2.8.2.2. Control.

> "Es un mecanismo que requiere atenuar el riesgo inherente, con el fin de reducir la probabilidad de ocurrencia y el impacto en caso de que dicho riesgo se materialice." (Deloitte, 2012)

2.8.2.3. Gestión de riesgos.

> "La gestión del riesgo proporciona un marco de referencia para la correcta administración de los riesgos asociados, con el fin de minimizar el impacto del riesgo en la empresa." (Deloitte, 2012)

La gestión del riesgo permite a las empresas:

- Mejorar la toma de decisiones como respuesta a los riesgos.
- Minimizar las pérdidas y los impactos operativos de los riesgos.
- Identificar y gestionar los riesgos en toda la organización
- Proporcionar respuestas adecuadas a los múltiples riesgos.

2.8.3. Identificación de activos.

Los activos de información de cada proceso o actividad analizada son identificados y clasificados de acuerdo a su criticidad (integridad, confidencialidad y disponibilidad) y a su vez los recursos críticos, son agrupados de acuerdo a sus funciones dentro de los procesos para posteriormente ser revisados a través de un ciclo continuo de valoración de riesgos para determinar las amenazas relevantes, las consecuencias de su materialización y la existencia y efectividad de controles implementados que disminuyen el impacto o la probabilidad de concretar la amenaza. (Torres, 2013, p. 73).

CAPÍTULO 3
ANÁLISIS DE LA DIRECCIÓN NACIONAL DE OPERACIONES DEL MINISTERIO DE FINANZAS

3.1. Antecedentes

La página web del Ministerio de Finanzas del Ecuador, en relación a su origen, establece que:

> "(…) se creó hace 181 años, en el marco de la naciente República del Ecuador, por lo que su historia refleja la leyenda de nuestro país, desde la perspectiva económica, básicamente de las cuentas públicas y de su principal instrumento de ejecución de política, que constituye el Presupuesto General del Estado". (Ministerio de Finanzas, 2013).

3.2. Misión

> "Innovar de manera permanente los conceptos, metodologías, procesos y servicios inherentes al Sistema Nacional de las Finanzas Públicas, para contribuir a una mayor eficiencia y efectividad en la gestión de las finanzas públicas". (Ministerio de Finanzas, 2013).

3.3. Visión

> "Garantizar la operación, seguridad y disponibilidad de la infraestructura tecnológica que soporta a las aplicaciones de software del sistema nacional de finanzas públicas en cumplimiento a los acuerdos de nivel de servicio establecidos". (Ministerio de Finanzas, 2013).

3.4. Funciones

Las principales funciones que cumple la Dirección Nacional de Operaciones se muestra en la siguiente tabla.

Tabla 3

Funciones de la Dirección Nacional de Operaciones

DIRECCIÓN NACIONAL DE OPERACIONES	
1	Garantizar que la infraestructura de tecnologías de información, satisfaga las necesidades de negocio del Sistema Nacional de las Finanzas Públicas (SINFIP) y los requerimientos técnicos de las aplicaciones.
2	Gestionar la disponibilidad, capacidad, continuidad de operaciones, seguridad e instalaciones de tecnología de información y de los sistemas del SINFIP.
3	Participar en la definición de SLAs.
4	Administrar la plataforma de hardware y software base.
5	Gestionar los problemas, cambios, configuración y versionado de plataforma.
6	Monitorear las operaciones y la producción de los sistemas.
7	Gestión de riesgos y de seguridad de infraestructura tecnológica de información y de los sistemas del SINFIP.

Fuente: Ministerio de Finanzas, Dirección de Talento Humano, 2014

3.5. Servicios

El menú de servicios que ofrece se resume en la siguiente tala.

Tabla 4

Servicios de la Dirección Nacional de Operaciones

	SERVICIOS
1	Portafolio de servicios de tecnología de la información.
2	Plan, políticas y reportes de seguridad de infraestructura.
3	Plan, líneas de base, umbrales, alarmas y base de datos de la capacidad de infraestructura.
4	Planes de continuidad y recuperaciones de operaciones correspondientes a tecnologías de información.
5	Plan de reducción de riesgo.
6	Plan, diseño y calendarios de la disponibilidad.
7	Plan de mantenimiento de las instalaciones.
8	Base de datos de gestión de la configuración actualizada.
9	Informe de administración técnica de contratos.

Fuente: Otorgada por el Ministerio de Finanzas

3.6. Descripción de aplicaciones

A continuación se realiza una breve descripción de las aplicaciones más críticas, que el Ministerio de Finanzas posee actualmente y que serán objeto principal de estudio del trabajo

3.6.1. Sistema eSigef.

El aplicativo denominado Sistema de Gestión Financiera, cuenta con los subsistemas de presupuesto y tesorería para cada ejercicio fiscal. Además utiliza para su seguridad un esquema de perfiles de usuarios que determinan los permisos sobre los objetos de aplicación. A continuación se detalla las siguientes definiciones:

- **Perfil:** El perfil es el agrupamiento de los objetos que tiene acceso para ejecutar una tarea específica.
- **Usuarios:** Es la definición final que reúne una o más funciones asignadas a una persona y otras características como el grupo de entidades a las que va a tener acceso.

Pantalla de inicio de sesión: Para acceder al sistema es necesario contar con un explorador o browser, cada usuario del sistema tendrá diferentes accesos, según las funciones asignadas.

Figura 10 Acceso de usuario

Fuente: Ministerio de Finanzas, recursos informáticos, 2014.

3.6.2. Sistema eSipren.

Dentro del sistema de administración de las Finanzas Públicas, se encuentra una de las aplicaciones denominada sistema presupuestario de remuneraciones y nómina, que permite validar la existencia del servidor público en el distributivo de remuneraciones, sueldos y salarios básicos aprobados por el Ministerio de Finanzas.

El acceso a este aplicativo se realiza de la siguiente manera:

Pantalla de inicio sesión: Para empezar a utilizar el sistema eSipren, se debe ingresar el nombre de usuario y la contraseña, otorgado por el administrador de usuarios del sistema.

Figura 11 Inicio de sesión

Fuente: Ministerio de Finanzas, recursos informáticos, 2014.

3.7. Elementos de infraestructura

Las capas que comprenden los servicios y funciones de los servidores que son monitoreados por la herramienta HP SITESCOPE se presentan en la siguiente tabla.

Tabla 5

Capas y servicios

Capas	Servicios
Presentación	En esta capa se encuentran los servicios IIS[9], controladores web. Realiza la función de presentar el aplicativo eSigef que está realizado en el lenguaje de programación .NET [10]
Aplicación	En esta capa funciona la lógica del negocio, además se encuentra código de programación correspondiente al aplicativo eSigef y eSipren.
Base de datos	En esta capa se encuentra el repositorio de datos con el gestor de base de datos Oracle versión 11g. Los equipos físicos correspondientes a esta capa mantienen un sistema operativo HP-UX[11].

Fuente: Ministerio de Finanzas, recursos informáticos, 2014.

Elaborado por: Wilman Sánchez

[9] Internet Information Server
[10] Framework de Microsoft
[11] Sistema operativo de alta disponibilidad, desarrollado por Hewlett-Packard

3.7.1. Elementos de configuración.

A continuación se presenta los dispositivos de hardware que deberán formar parte de la infraestructura de los servicios a ser monitoreados.

3.7.2. Elementos de hardware.

Los dispositivos de hardware correspondientes a la infraestructura tecnológica de los servidores del Ministerio de Finanzas son:

- Servidores
- Routers
- Firewalls
- Balanceadores
- Dispositivo de almacenamiento

3.7.2.1. Servidores.

Los servidores que conforman la infraestructura tecnológica de los servicios eSigef, eSipren y de monitoreo, se dividen de acuerdo a las capas del diseño de infraestructura correspondientes, se describen en la siguiente tabla.

Tabla 6

Servidores correspondientes a la infraestructura tecnológica

Capa Presentación		
Nombre	**Sistema Operativo**	**Características Técnicas**
ePRE01p	Windows server versión 2003 versiones de 32 y 64 bits.	HP Proliant BL46oc Generation 6 (g6) Server Blade. Procesador Intel Xeon X556O. RAM: 6 paletas x 2 GB
ePRE02p		
ePRE03p		
ePRE60p		
ePRE61p		

Capa Presentación		
Nombre	**Sistema Operativo**	**Características Técnicas**
ePRE01p	Windows server versión 2003 versiones de 32 y 64 bits.	HP Proliant BL46oc Generation 6 (g6) Server Blade. Procesador Intel Xeon X556O. RAM: 6 paletas x 2 GB
ePRE02p		
ePRE03p		
ePRE60p		
ePRE61p		

Capa Aplicación		
Nombre	**Sistema Operativo**	**Características Técnicas**
eAPP01p	Windows server versión 2003 versiones de 32 y 64 bits.	Tipo: HP Proliant BL46oc Generation 6 (g6) Server Blade. Procesador: Intel Xeon X556O. RAM: 6 paletas x 2 GB
eAPP02p		
eAPP03p		
eAPP60p		
eAPP61p		
Capa Base de Datos		
Nombre	**Sistema Operativo**	**Características Técnicas**
eBDD01p eBDD02p	HP UX	Tipo: HP Integrity rx 7640 Server. Arquitectura: EPIC. ITANIUM 2 de 64 bits nativos. El procesador: Intel Dual-core Itanium Discos duros : 4 - Capacidad de cada disco: 146 GB con velocidad interna: 15 000 rpm
Monitoreo		
Nombre	**Sistema Operativo**	**Características Técnicas**
SITESCOPE	Windows server versión 2003 versión estándar	Procesador Intel Xeon X5650 de 2.67 GHz. RAM: 4 GB

Fuente: Ministerio de Finanzas, recursos informáticos, 2014.

Nota: El identificador **ePRE01p** representa a un servidor correspondiente a la capa presentación y la numeración **01, 02, 03**, corresponden al número secuencial asignado a cada uno servidores que conforman esta capa.

El identificador **eAPP01p** representa a un servidor correspondiente a la capa aplicación y la numeración **01, 02, 03**, corresponde al número secuencial asignado a cada uno servidores que conforman esta capa.

El identificador **eBDD01p** representa a un servidor correspondiente a la capa de base de datos y la numeración **01, 02,** corresponde al número secuencial asignado a cada uno servidores que conforman esta capa.

El identificador **SITESCOPE** corresponde al servidor donde se encuentra alojada la herramienta de monitoreo, la cual se encargará de monitorear las 3 capas de infraestructura de los servicios eSigef y eSipren.

3.7.2.2. Routers. [12]

Los routers que conforman la infraestructura tecnológica de los servicios eSigef, eSipren y de monitoreo se presentan en la tabla siguiente.

Tabla 7

Routers

Nombre	Tipo	RAM
Ro01	Catalyst 3560	2000 MB
Ro02	Link Controller	1794 MB

Fuente: Ministerio de Finanzas, recursos informáticos, 2014.

Nota: El identificador **R**, representa a un dispositivo Router y la numeración **01, 02,** corresponde al número secuencial asignado a cada Router que conforman esta capa.

3.7.2.3. Firewalls de red.

Los firewalls de red que conforman la infraestructura tecnológica de los servicios eSigef, eSipren y de monitoreo, se describen en la siguiente tabla.

Tabla 8

Firewalls

Identificador	Nombre	Tipo	RAM	CPU
FW01	eFW-5540-EXT	CISCO ASA 5540	2048 MB	Pentium 4 2000 MGHz
FW02	eFW-5580-DAT	CISCO ASA 5580	8192 MB	AMD Opteron 2600 MHz.

Fuente: Ministerio de Finanzas, recursos informáticos, 2014.

Nota: El identificador **FW**, representa a un dispositivo tipo firewall y la numeración **01, 02,** corresponden al número secuencial asignado a cada firewall que conforman esta capa.

3.7.2.4. Balanceadores de red.

Los balanceadores de red que conforman la infraestructura tecnológica de los servicios eSigef, eSipren y de monitoreo se presentan a continuación.

[12] Router: enrutador o encaminador de paquetes

Tabla 9

Balanceadores de red

Identificador	Nombre	Tipo
B01	AC.com	BIG-IP
B02	AC.com	BIG-IP

Fuente: Ministerio de Finanzas, recursos informáticos, 2014.

Nota: El identificador **B**, representa a un dispositivo tipo balanceadores y la numeración **01, 02,** corresponden al número secuencial asignado a cada balanceador que conforman esta capa.

3.7.2.5. Dispositivo de almacenamiento.

El dispositivo de almacenamiento que ayuda a la capa de base de datos a realizar el almacenamiento corporativo de los datos que ingresan a los servicios eSigef, eSipren, se presenta en la siguiente tabla.

Tabla 10

Dispositivo de almacenamiento

Identificador	Tipo	Componentes
AL01	HP Storage Works XP20000	Controladoras de configuración: Activo/Activo.
		Discos: 32 GB de memoria cache instalada.
		16 puertos Fiber Channel de 4Gbps para conexión con la red de almacenamiento SAN.
		128 discos Fiber Channel (FC) Dual Port de 4Gbps con 15000 rpm de velocidad y 450GB de capacidad.
		8 discos de 2TB SATA Dual Port de 7200 rpm incluye 2 discos de similares características para la función de spare.

Fuente: Ministerio de Finanzas, recursos informáticos, 2014.

Nota: El identificador **AL**, representa a un dispositivo de almacenamiento y la numeración **01**, corresponde al número de dispositivo de almacenamiento que existe para esta capa.

3.7.3. Elementos de configuración de software.

El software correspondiente a la infraestructura tecnológica del Ministerio de Finanzas, que es administrado por la Dirección Nacional de Operaciones, se describe a continuación

3.7.3.1. Sistemas operativos base.

La tabla que se presenta a continuación, muestra los sistemas operativos base, instalados en los servidores que corresponden a la infraestructura tecnológica del centro de datos.

Tabla 11

Sistemas operativos base

Identificador	Tipo
SO01	Windows Server 2003 R2
SO02	Red Hat Linux versión 6.5

Fuente: Ministerio de Finanzas, recursos informáticos, 2014.

Elaborado por: Wilman Sánchez

Nota: El identificador **SO**, representa al tipo de sistema operativo que utilizan los servidores y la numeración **01, 02,** corresponde al número de sistemas operativos existentes.

3.7.3.2. Sistema gestor de base de datos (SGBD).

En la tabla siguiente se muestra el tipo de sistema gestor de base de datos, instalado en los servidores de la capa de base de datos correspondiente a la infraestructura tecnológica del centro de datos.

Tabla 12

Sistema gestor de base de datos

Identificador	Tipo
ORA01	ORACLE 11G Release 2 versión 11.0.2

Elaborado por: Wilman Sánchez

Nota: El identificador **ORA**, representa al sistema gestor de base de datos que utilizan los servidores para el almacenamiento de datos y la numeración **01** corresponde al número de sistema gestor de base de datos existentes.

3.7.3.3. Servicios web.

Los servicios web de la infraestructura tecnológica del centro de datos se presentan en la tabla siguiente.

Tabla 13

Servicios Web

Identificador	Tipo
SWB01	IIS versión 6.0
SWB02	Framework .NET

Fuente: Ministerio de Finanzas, recursos informáticos, 2014.

Elaborado por: Wilman Sánchez

Nota: El identificador **SWB**, representa al servicio web que utilizan los servidores y la numeración **01, 02** corresponde al número de servicios web existentes.

3.7.3.4. Software de monitoreo.

El software instalado para el monitoreo de infraestructura de los servicios eSigef y eSipren se muestra en la siguiente tabla.

Tabla 14

Software de monitoreo

Identificador	Tipo
SM01	HP Sitescope versión 10.12

Fuente: Ministerio de Finanzas, recursos informáticos, 2014.

Elaborado por: Wilman Sánchez

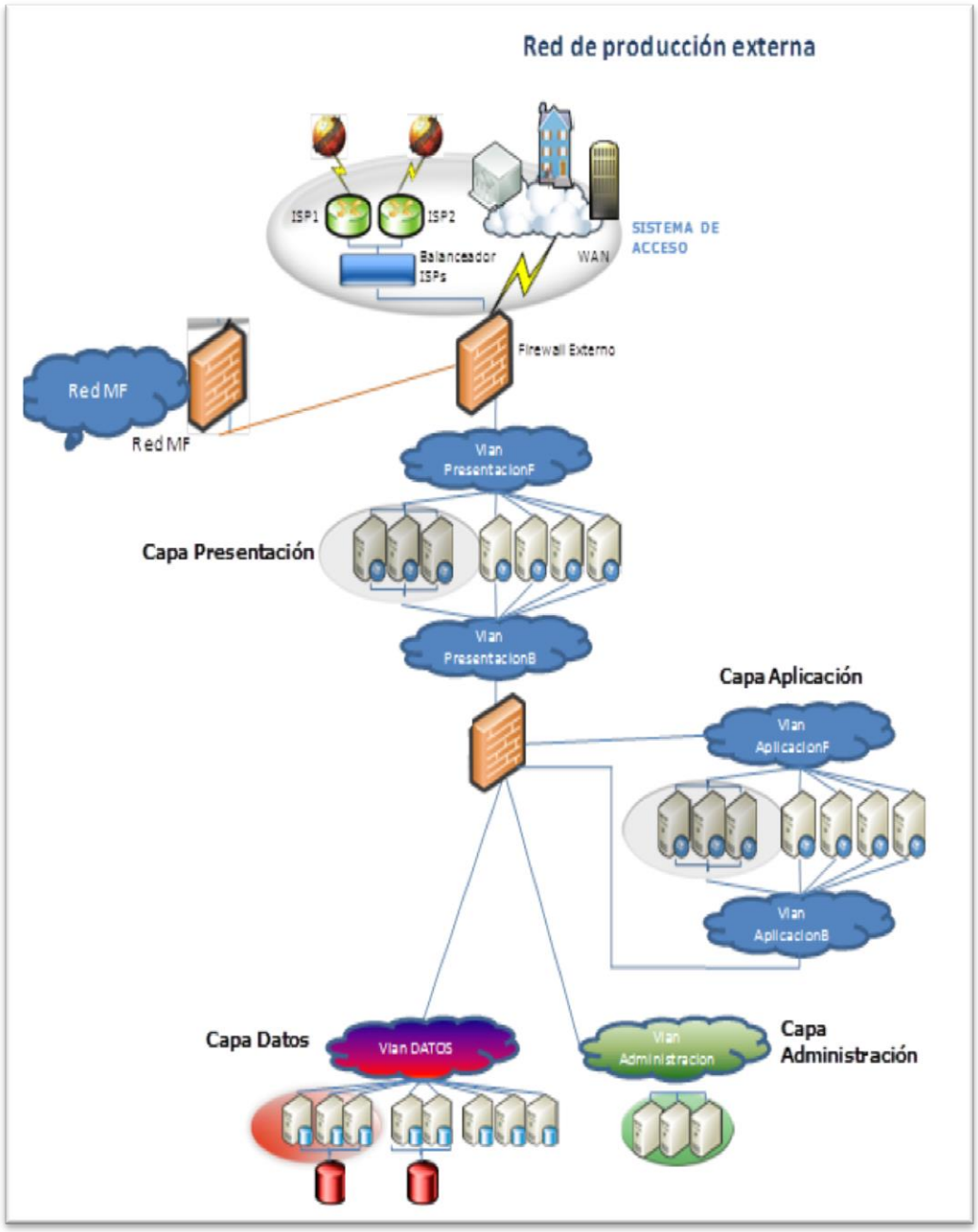
Nota: El identificador **SM**, representa software de monitoreo y la numeración **01** corresponde al número de softwares de monitoreo existentes.

3.8. Infraestructura tecnológica

El Ministerio de Finanzas mantiene una arquitectura basada en capas con alta disponibilidad en la infraestructura de sus servidores ya que posee 3 servidores por capa. La interconexión de la infraestructura tecnológica de los servicios eSigef y eSipren comprenden las capas de: presentación, aplicación y datos (incluye la capa de administración de servidores).

El acceso a los servicios del Ministerio de Finanzas se realiza mediante un firewall externo que conecta con la capa de presentación. La capa de aplicación y la capa de datos comparten un firewall interno, adicionalmente y con el objetivo de administrar los servidores, existe la capa de administración, por la cual de manera remota se puede acceder a cada uno de los servidores.

Figura 12 Esquema de interconexión actual

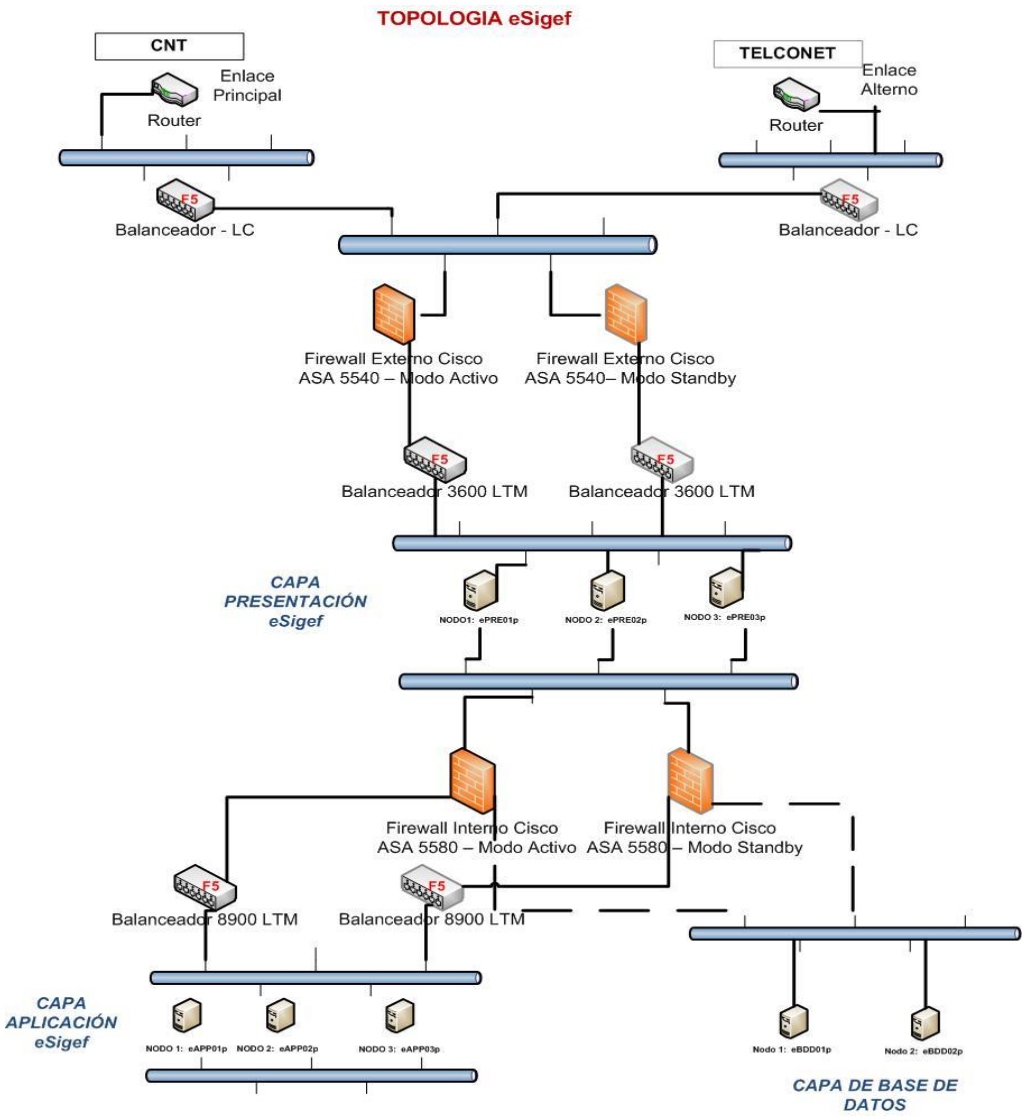


Fuente: Ministerio de Finanzas, recursos informáticos, 2014.

3.8.1. Representación de la infraestructura del aplicativo eSigef.

La figura que se presenta después de éste párrafo muestra el diagrama lógico de red, donde se puede apreciar a cada una de las capas que conforman el aplicativo eSigef del Ministerio de Finanzas.

Figura 13 Representación del diagrama lógico del aplicativo eSigef



Fuente: Ministerio de Finanzas, recursos informáticos, 2014.

En la figura se observa que existen dos proveedores del servicio de internet (CNT [13] y TELCONET[14]) que acceden hacia la capa de presentación del eSigef la cual está

[13] Corporación Nacional de Telecomunicaciones

protegida por dos firewalls externos marca CISCO[15], modelo ASA [16] 5540 operando en el esquema de Activo, lo que significa que uno de los dos firewalls en condiciones normales operará como firewall activo y el otro como firewall standby, que ayudan a la seguridad en esta capa. Además existen 2 balanceadores para esta capa, modelo 3600 LTM, con el objetivo de balancear las peticiones de los servicios en los servidores y enlaces; debido a que estos equipos proporcionan mayor robustez a las aplicaciones y disponibilidad de las mismas.

Para acceso a la capa de aplicación es similar a las características de seguridad que la capa de presentación, cuenta con dos firewalls ASA de modelo ASA 5580 operando en el esquema activo y espera, los detalles de operación fueron descritos anteriormente. También existe 2 balanceadores modelo 8900 los cuales proporcionan mayor robustez y disponibilidad a esta capa.

3.8.2. Representación de la infraestructura del aplicativo eSipren.

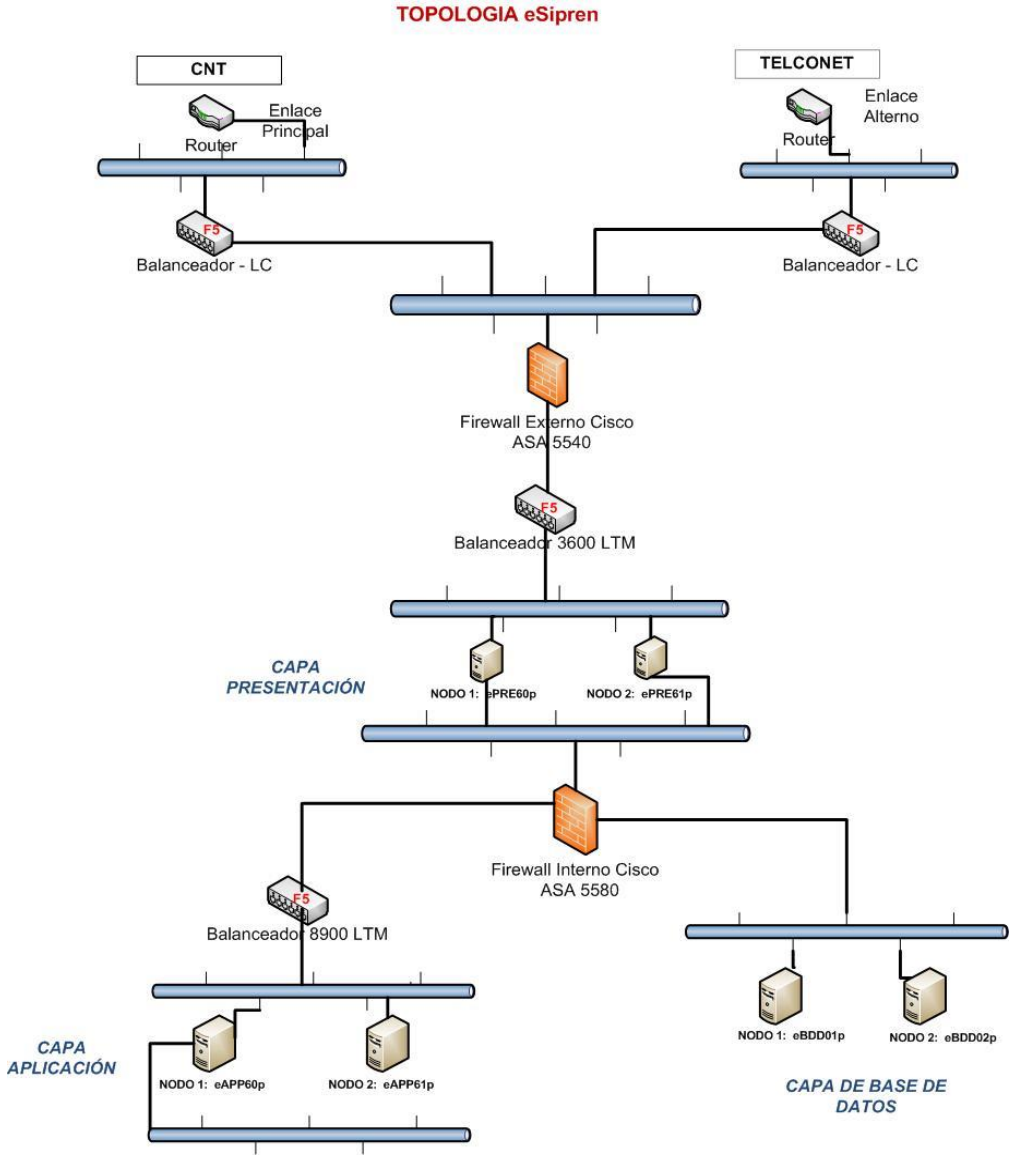
La infraestructura del aplicativo eSipren se la puede definir como un diagrama lógico de red donde se detalla la interconexión de cada una de las capas que conforman la red del aplicativo en el Ministerio de Finanzas y la forma en que interconectan los equipos.

Conforme se presenta más adelante en la figura denominada "Diagrama lógico del aplicativo eSipren" existen dos proveedores del servicio de internet (CNT y TELCONET) que acceden hacia la capa de "presentación", la cual está protegida por un firewall externo marca CISCO, modelo ASA 5540, operando en el esquema de Stateful Failover Activo, que ayuda a la seguridad en esta capa. Además un balanceador para esta capa, modelo 3600 LTM, para tener equilibrio de sus servidores y enlaces, debido a que este equipo proporciona mayor robustez a las aplicaciones y disponibilidad.

[14] Proveedor de Internet
[15] CISCO: Empresa global dedicada a la fabricación, venta, mantenimiento y consultoría de equipos de telecomunicaciones.
[16] Firewall de la marca CISCO

El acceso a la capa de aplicación es similar a las características de seguridad de la capa "presentación", cuenta con un firewall ASA de modelo ASA 5580 y un balanceador modelo 8900, los cuales proporcionan mayor robustez y disponibilidad.

Figura 14 Diagrama lógico del aplicativo eSipren



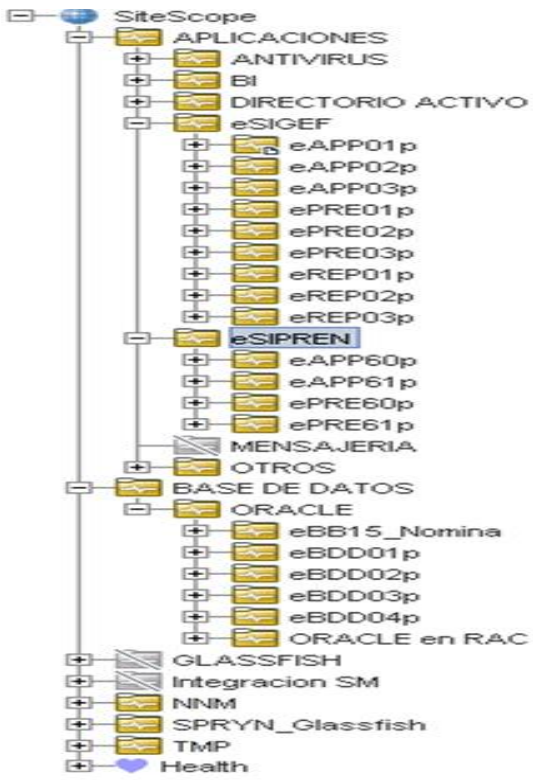
Fuente: Ministerio de Finanzas, recursos informáticos, 2014.

La capa de base de datos, comparte los firewalls de la capa aplicación del eSigef, no posee balanceados físicos existentes en las capas presentación y aplicación.

3.8.3. Servidores ingresados en HP SITESCOPE.

En los servidores, la herramienta HP SITESCOPE, realizará el monitoreo de las carpetas identificadas con las aplicaciones eSigef y eSipren, conforme se ilustra en la siguiente figura.

Figura 15 Servidores ingresados al monitoreo en HP SITESCOPE

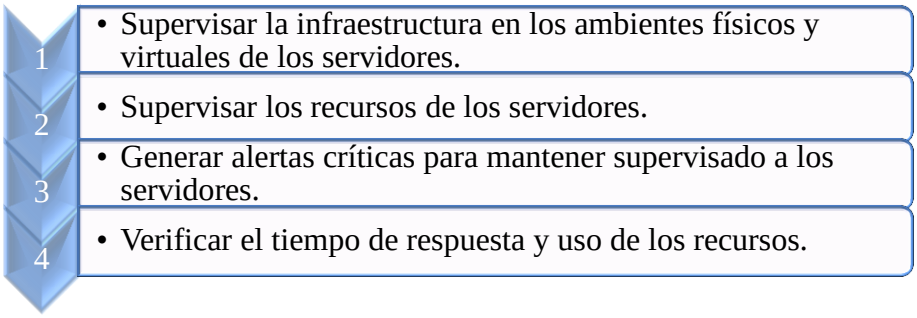


Fuente: Ministerio de Finanzas, Dirección de Operaciones, 2014.

3.9. Funciones de monitorización hacia los servidores

En la siguiente figura se presenta las funciones de monitorización dirigidas a los servidores.

Figura 16 Función de monitorización



Elaborado por: Wilman Sánchez

En el monitoreo de los servidores se incluyen:

- CPU utilización Monitor.
- Disk Space monitor.
- Memory monitor.
- Network monitor.
- Web Server monitor.

3.10. Situación actual de la infraestructura tecnológica de los servidores

Este análisis ayudará a conocer cuáles son los factores que afectan a la disponibilidad de los servidores para poder sustentar la propuesta de monitoreo que se realizará en el capítulo 4 del trabajo.

3.10.1. Recopilación de información.

La recopilación de información se realizó a través de encuestas con preguntas de tipo cerradas a los administradores de servidores, base de datos y comunicaciones. También las observaciones tomadas durante las visitas realizadas a la institución, durante los meses de noviembre 2013 y enero del 2014.

- **Personal a ser entrevistado**

Debido al tipo de información a ser recopilada es importante que el personal técnico de la Dirección Nacional de Operaciones entrevistado sea del nivel administrador.

Tabla 15

Administradores encuestados

Encuestado	Rol	Grado	Descripción
Ing. Nelson Echeverría	Administrador de servidores	Servidor Público 7	La entrevista, se la realizó en una reunión el día 4 de noviembre del 2013
Ing. Edison Calero	Administrador de base de datos	Servidor Público 7	La entrevista, se la realizó en una reunión el día 11 de noviembre del 2013
Ing. Paul Guerrero	Administrador de comunicaciones	Servidor Público 7	La entrevista, se la realizó en una reunión el día 6 de enero del 2014

Elaborado por: Wilman Sánchez

- **Activos de infraestructura a ser tomados en cuenta**

Entre los activos que se consideran de vital importancia dentro de la infraestructura correspondiente a los servicios eSigef y eSipren son:

Tabla 16

Activos importantes

Activo	Características
Servidores	Correspondientes a las 3 capas que conforman los servicios eSigef y eSipren, incluyendo la herramienta de monitoreo.
Routers, firewalls, balanceadores	Elementos correspondientes a la infraestructura tecnológica de la red interna de los servicios eSigef y eSipren.
Unidad de almacenamiento	Elemento correspondiente a la capa de base de datos, donde se aloja la información de los servicios.
Sistemas operativos	Tipos de sistemas operativos base, instalados en los servidores.
Sistema de gestión de base de datos	Sistema que permite el almacenamiento, modificación, administración de base de datos Oracle.
Servicios web	Tecnología usada para el intercambio de datos entre aplicaciones
Personal	Personal técnico de nivel administrador correspondiente a la infraestructura tecnológica de los servicios eSigef y eSipren.

Elaborado por: Wilman Sánchez

- **Procesos ITIL a ser considerados**

De acuerdo a la investigación realizada sobre ITIL, se deduce que existe una estrecha relación entre la monitorización de infraestructura y la gestión de la disponibilidad y la Gestión de Eventos. Los parámetros definidos en ITIL, realizan ajustes y definen nuevos procedimientos a fin de mejorar el monitoreo que se realiza en la Dirección Nacional de Operaciones, de manera que permita:

- Ajustar los planes de disponibilidad a las necesidades reales del negocio.
- Disponer de toda la información necesaria sobre la infraestructura como las interrupciones del servicio, estadísticas de uso, etc.
- Monitorizar los eventos importantes ocurridos en la infraestructura de los servicios.

Estos factores permitirán relacionar y verificar el cumplimiento de los procesos de gestión de disponibilidad y de eventos de acuerdo a las mejores prácticas del marco de referencia ITIL V3.

- **Gestión de Disponibilidad**

Este proceso ha sido tomado en cuenta debido a que es necesario monitorizar la disponibilidad de infraestructura, la cual abarca la mayoría de elementos que son importantes para la operación normal de los servicios, por ejemplo, en caso de que llegará a producirse un daño en un servidor de correo electrónico, afectaría la disponibilidad del servicio de correo que es de vital importancia para los empleados de una empresa.

- **Gestión de Eventos**

Este proceso es tomado en cuenta debido a que se encarga de monitorear todos los eventos que ocurren en la infraestructura para permitir su operación normal a través de la detección oportuna.

Un evento se lo define como cualquier suceso detectable que sea significativo para la gestión de la infraestructura y servicios. En consecuencia, una gestión de eventos depende del conocimiento del estado de la infraestructura a través de la detección oportuna de cualquier comportamiento que cause la operación anormal de un elemento para lo cual existen en el mercado sistemas monitoreo de dos tipos: (IBM, 2014) .

a) **Sistemas de monitoreo activo**: verifican la infraestructura para determinar el estado y disponibilidad de los elementos críticos. Cualquier excepción generará una alerta que necesita ser comunicada a la herramienta o equipo adecuado para tomar acciones correspondientes.

b) **Sistemas de monitoreo pasivo:** detectan y correlacionan alertas operacionales y de comunicación generadas por la infraestructura.

3.10.2. Indicadores a ser evaluados de acuerdo a la norma.

Los procesos de gestión de disponibilidad y eventos, son aquellos que poseen relación con actividades de monitoreo que realiza la herramienta HP SITESCOPE, para esto serán evaluados los indicadores en relación con ITIL V3, que luego harán referencia a la formulación de encuestas realizadas a los administradores de infraestructura.

A la hora de evaluar la eficiencia y efectividad de los procesos de gestión de disponibilidad y eventos, deben verificarse los indicadores que se describen en la tabla del siguiente numeral.

- **Gestión de Disponibilidad**

Para evaluar la gestión de disponibilidad se deben aplicar los indicadores que se presentan en la siguiente tabla.

Tabla 17

Indicadores de disponibilidad

Proceso	Indicadores
Gestión de Disponibilidad	• Porcentaje de disponibilidad de los servicios. • Cantidad de interrupciones de servicio. • Duración media de interrupciones de servicio. • Porcentaje de servicios y componentes de infraestructura sujetos a monitorización de disponibilidad. • Cantidad de medidas implementadas con el objetivo de aumentar la disponibilidad.

Fuente: (Osiatis, 2011)
Elaborado por: Wilman Sánchez

Descripción:

Con respecto a los indicadores para obtener un valor de referencia se usa el punto "Porcentaje de disponibilidad de los servicios", luego para obtener una estadística del número de caídas del servicio ocurridas durante un periodo de tiempo se diseñan los indicadores: "Cantidad de interrupciones de servicio", "Duración media de interrupciones de servicio".

Además, con el objetivo de monitorizar y aumentar la disponibilidad de infraestructura, se añade los siguientes indicadores: "Porcentaje de servicios y componentes de infraestructura sujetos a monitorización de disponibilidad" y "Cantidad de medidas implementadas con el objetivo de aumentar la disponibilidad".

- **Gestión de Eventos**

ITIL recomienda en la Gestión de Eventos medir los eventos ocurridos en la infraestructura, para esto se añade los indicadores: "Número de eventos, por categorías"," Número de eventos, por importancia". Es necesario la medición de los eventos que tengan problemas con el rendimiento de los equipos de infraestructura para esto se añade el indicador "Número de eventos relacionados con problemas de rendimiento", con el objetivo de disminuir los problemas que pueden ocurrir en los eventos ocasionados a futuro se tiene el indicador de "Número de eventos que indican futuros problemas de disponibilidad".

Tabla 18

Indicadores de eventos

Proceso	Indicadores
Gestión de Eventos	• Número de eventos, por categorías. • Número de eventos, por importancia. • Número de eventos relacionados con problemas de rendimiento. • Número de eventos que indican futuros problemas de disponibilidad. • Número de cada tipo de evento por plataforma o aplicación.

Fuente: (Osiatis, 2011)
Elaborado por: Wilman Sánchez

Además cada aplicación se comporta diferente dependiendo del número de usuarios que accedan a la misma, así como también de la infraestructura que posea, para esto se añade el indicador: "Número de cada tipo de evento por plataforma o aplicación".

3.10.3. Evaluación de indicadores.

Para la evaluación coherente de los indicadores se realizaron encuestas a los administradores de infraestructura, se utilizaron los siguientes factores:

- Ponderado
- Número de cumplimiento
- Cálculo de probabilidad de amenaza por indicador
- Cumplimiento de indicadores

3.10.3.1. Porcentaje de cumplimiento (número de cumplimiento).

Previo a obtener el valor del cumplimiento se realiza la suma del número total de respuestas realizadas a las encuestas. Para realizar el cálculo del porcentaje total de respuestas se utiliza la siguiente formula:

#Total = (# Resp. Correctas + # Resp. Incorrectas + # Resp. NA)*100

El ponderado de respuestas a las preguntas realizadas con respecto a los indicadores se calcula con la siguiente formula.

#Ponderado = (# Resp. Correctas * 100 + (# Resp. Incorrectas + # Resp. NA)* 0)

Luego de haber realizar el cálculo del total de respuestas y el ponderado, se procede a calcular el porcentaje de cumplimiento para cada indicador. Con la siguiente ecuación se logra obtener el nivel de cumplimiento para cada indicador.

$$\textbf{\#Cumplimiento} = \frac{\#\text{Ponderado}*100}{\#\text{total}}$$

Dónde:

Indicador_Total = La suma de los indicadores evaluados a cada administrador de infraestructura para este caso son 3 administradores.

El cumplimiento es obtenido mediante el valor del ponderado a las preguntas por un valor de 100 dividido para el valor total de respuestas contestadas de acuerdo a la percepción en labores diarias en la Dirección Nacional de Operaciones.

El cálculo de las formulas **#Total, #Ponderado, #Cumplimiento** se relacionan con el libro de Magerit, en su capítulo donde se evalúan los indicadores de estudio de tecnología. (MHAP, 2012)

3.10.3.2. Cálculo del porcentaje de probabilidad de amenaza.

Para calcular el porcentaje de probabilidad de amenaza, es necesario aplicar la fórmula de **Prob. Amenaza**. Debido a que el resultado encontrado implica la probabilidad de que una amenaza ocurra.

Para calcular el porcentaje de probabilidad de una amenaza se relaciona con el porcentaje del cumplimiento de la percepción de los indicadores evaluados, en las encuestas hacia los administradores de la infraestructura, por tanto la ecuación para el cálculo es:

$$\textbf{Prob. Amenaza} = \frac{100 - \#\text{Cumplimiento}}{100}$$

Dónde:

100 = Valor meta de cumplimiento

Cumplimiento = Valor obtenido del nivel de cumplimiento de cada una de las preguntas realizadas a los administradores de la infraestructura.

Mientras el valor de la probabilidad de amenaza se acerque a 1 (valor máximo), es mayor la probabilidad de que una amenaza se materialice, caso contrario mientras el valor de la probabilidad de amenaza tienda a 0, la probabilidad es nula.

3.10.3.3. Interpretación de cumplimiento de indicadores.

Para determinar el cumplimiento de los indicadores se utilizó el rango de valores de la tabla 20, establecido por contraloría interna del Ministerio de Finanzas, con el fin de identificar el grado de confianza del cumplimiento de los indicadores.

Este tipo de auditorías se toma como referencia las normas que rige el Ministerio de Finanzas como institución pública, con respecto a las medidas dispuestas por Contraloría General del Estado.

En las dos tablas siguientes se presentan la interpretación y grados de confianza sobre el cumplimiento de indicadores.

Tabla 19

Interpretación de cumplimiento de indicadores

#Cumplimiento	Grado de confianza
15 – 50	B
51 – 59	MB
60 – 66	MM
67 – 75	MA
76 – 95	A

Fuente: Ministerio de Finanzas, Dirección de Operaciones, 2014.

El cumplimiento contempla 5 rangos a los cuales les corresponde un grado de confianza conforme a lo establecido por Contraloría Interna del Ministerio de Finanzas:

Tabla 20

Grados de confianza

Sigla	Grado de confianza
B	Bajo
MB	Moderado bajo
MM	Moderado
MA	Moderado alto
A	Alto

Fuente: Ministerio de Finanzas, Dirección de Operaciones, 2014.

El cumplimiento del 15% hasta un 50% es considerado como un grado de confianza Bajo, esto se presenta cuando una actividad es cumplida en parte o hasta la mitad. El grado de confianza Moderado Bajo es catalogado como moderado por estar en el valor del 50% del grado de confianza. El valor MB implica que una actividad se la realiza al menos un poco más de la mitad pero aún no es satisfactoria. El grado de confianza Moderado se encuentra desde el 60% hasta 66% de cumplimiento y se lo califica como regularmente satisfactorio. Un grado de confianza Moderado Alto posee el rango más alto de confianza del 67% a 75% satisfactorio. Mientras el grado de confianza entre el rango del 76% a 95% que corresponde al grado de confianza Alto, posee la calificación más alta al evaluar las actividades de tecnología; por estar encima del rango moderado y cerca del 100% posee una calificación satisfactoria.

En caso de existir un porcentaje de cumplimiento entre los valores 0% a 14% se tendrá un grado de confianza bajo y el porcentaje de cumplimiento de los valores comprendidos entre el 96% a 100% será alto, son considerados como ideales.

Para mantener el estándar que la Contraloría General del Estado proporciona se asume al rango inferior como un grado confianza bajo y al grado de confianza superior se lo incorporó con el grado de confianza alto.

3.10.4. Formulación de resultados.

A continuación se presenta el detalle de las encuestas con respecto a la Gestión de Disponibilidad y de eventos los cuales están relacionados con el monitoreo de infraestructura, las respuestas a las encuestas realizadas se obtuvieron según la percepción de los administradores de infraestructura involucrados. Después de detallar estos factores se mostrará el resultado del análisis de riesgos.

3.10.4.1. Gestión de la Disponibilidad.

Los administradores de la infraestructura de acuerdo a su percepción, presentan los resultados con respecto al porcentaje de cumplimiento en la gestión de disponibilidad.

Tabla 21

Encuestas sobre la Gestión de Disponibilidad

Ítem	Preguntas	Administrador de Servidores			Administrador de BDD			Administrador de Comunicaciones		
		Si	No	N/A	Si	No	N/A	Si	No	N/A
1	¿Se monitorea la disponibilidad de los servicios en relación a la disponibilidad acordada?		X			X		X		
2	¿Se monitorea la cantidad de interrupciones de servicio ocurridas?		X		X			X		
3	¿Existe el monitoreo de duración media de interrupciones de un servicio?		X		X			X		
4	¿Se monitorea el porcentaje de servicios y componentes de infraestructura sujetos a monitorización de disponibilidad?		X			X			X	

Elaborado por: Wilman Sánchez

Ítem	Preguntas	Administrador de Servidores			Administrador de BDD			Administrador de Comunicaciones		
		Si	No	N/A	Si	No	N/A	Si	No	N/A
5	¿Se posee el conocimiento de la cantidad de medidas implementadas con el objetivo de aumentar la disponibilidad?		X			X			X	

Elaborado por: Wilman Sánchez

Cálculo de indicadores para Gestión de Disponibilidad

A continuación se muestra un resumen del cálculo de las preguntas de la Gestión de Disponibilidad descritas en la tabla anterior, a fin de calcular el nivel de cumplimiento y la probabilidad de amenaza para cada una de las preguntas, estas se relacionan con los indicadores de disponibilidad descritos en la tabla 17.

Tabla 22

Resumen de cálculo de indicadores

# Pregunta	#Total	#Ponderado	#Prob. Amenaza	#Cumplimiento
1	300	100	0.66	33.33
2	300	200	0.33	66.66
3	300	200	0.33	66.66
4	300	0	1	0
5	300	0	1	0
Promedio del cumplimiento				33.33

Elaborado por: Wilman Sánchez

Indicadores de disponibilidad

Más del 50 % de los indicadores poseen un nivel de cumplimiento bajo, esto implica que no existe un monitoreo deseable para prevenir inconvenientes que puedan presentarse a futuro con respecto a la disponibilidad infraestructura de los servicios eSigef y eSipren.

Es necesario para efectos de mejorar la monitorización de la disponibilidad de la infraestructura que por lo menos se lleve una bitácora actualizada de información de la infraestructura de la organización, además se cuenta con un mapa de la topología de los elementos configurables para que así sean monitoreados elementos como: los CPUs que contienen cada servidor, monitoreo de memoria RAM, capacidad en disco local, tarjetas de red del equipo configurable, que pertenecen a la infraestructura.

Tabla 23

Grado de confianza de disponibilidad realizadas por los administradores

N°. pregunta	#Cumplimiento	Grado de confianza
4	0	B
5	0	B
1	33.33	B
2	66.66	MA
3	66.66	MA

Elaborado por: Wilman Sánchez

La mayoría de indicadores evaluados poseen un grado de confianza bajo, este valor está relacionado con la falta de monitoreo a la disponibilidad de los servicios, siendo necesario se cuente con una herramienta tecnológica de monitoreo que ayude a solucionar estos problemas que a futuro pueden convertirse en críticos ya que pueden disminuir la disponibilidad de los servicios tecnológicos del Ministerio de Finanzas.

3.10.4.2. Gestión de Eventos.

En la siguiente tabla se presenta la percepción de los administradores de la infraestructura sobre la Gestión de Eventos.

Tabla 24

Encuestas sobre la Gestión de Eventos

Ítem	Preguntas	Administrador de Servidores			Administrador de BDD			Administrador de Comunicaciones		
		Si	No	N/A	Si	No	N/A	Si	No	N/A
1	¿Se monitorea el número de eventos, por categorías?		X			X		X		
2	¿Existe un monitoreo del número de eventos, por importancia?		X				X	X		
3	¿Se monitorea el número de eventos relacionados con problemas de rendimiento?		X		X				X	
4	¿Existe un monitoreo del número de eventos que indican futuros problemas de disponibilidad?		X		X				X	
5	¿Existe un monitoreo del tipo de evento, por aplicación?		X		X					X

Elaborado por: Wilman Sánchez

Cálculo de indicadores para Gestión de Eventos

A continuación se muestra un resumen del cálculo de las preguntas de la Gestión de Eventos con la finalidad de establecer el nivel de cumplimiento y la probabilidad de amenaza para cada una de las preguntas formuladas.

Tabla 25

Resumen de cálculo de indicadores

# Pregunta	#Total	#Ponderado	#Prob. Amenaza	#Cumplimiento
1	300	100	0.66	33.33
2	300	100	0.66	33.33
3	300	100	0.66	33.33
4	300	100	0.66	33.33
5	300	100	0.66	33.33
Promedio del cumplimiento				33.33

Elaborado por: Wilman Sánchez

Indicadores de eventos

Casi todos los indicadores evaluados para la Gestión de Eventos poseen un nivel de cumplimiento bajo, esto implica una carencia que se relaciona con la monitorización, la falta de una herramienta tecnológica y la planificación.

Para mejorar la monitorización de los eventos ocurridos en la infraestructura de los servicios eSigef y eSipren se necesita disponer de al menos una herramienta que monitorice todo el tiempo cualquier evento que se genere en la infraestructura ya sea por el consumo excesivo o la configuración de los servidores (CPU, Memoria, Disco).

Tabla 26

Grado de confianza de incidentes

N°. pregunta	#Cumplimiento	Grado de confianza
1	33.33	B
2	33.33	B
3	33.33	B
4	33.33	B
5	33.33	B

Elaborado por: Wilman Sánchez

Todos los indicadores evaluados poseen un grado de confianza bajo el cual se relaciona con la falta de una herramienta de monitoreo que automatice la Gestión de Eventos, por lo que es necesario que HP SITESCOPE sea implementada como herramienta de monitoreo en la Dirección Nacional de Operaciones, con el objetivo de que estos niveles de cumplimiento actualmente obtenidos aumenten a un grado considerable y que a futuro no puedan afectar la disponibilidad de los servicios eSigef y eSipren que son considerados los más importantes para el Ministerio de Finanzas.

3.10.5. Evaluación de riesgos.

En este punto se realiza la evaluación de riesgos de los indicadores mencionados en las tablas 17 y 18 del trabajo de investigación.

3.10.5.1. Método de evaluación.

El método base a ser usado es MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información). La técnica a utilizar será mediante el análisis de tablas debido a que se adapta mejor a los indicadores que se manejan en el presente trabajo de titulación.

Impacto

Implica cuál sería el nivel de gravedad en caso de que ocurra una amenaza, esta puede variar según la naturaleza del impacto.

Estimación del impacto

Se puede calcular el impacto en base a tablas sencillas de doble entrada como se muestra a continuación:

Tabla 27

Estimación de impacto[17]

impacto		degradación		
		1%	10%	100%
valor	MA	M	A	MA
	A	B	M	A
	M	MB	B	M
	B	MB	MB	B
	MB	MB	MB	MB

Fuente: (Ministerio de Administraciones Públicas, 2005)

Aquellos activos que reciban una calificación de impacto muy alto (MA) deberían ser objeto de atención inmediata.

La escala que sugiere MAGERIT para calificar el riego es de 5 peldaños, es decir en una escala del 1 al 5, los mismos que se representan por un estado de riesgo.

Tabla 28

Calificación de los impactos ocurridos según el estándar MAGERIT

Riesgo	Estado de riesgo	Siglas
1	muy bajo	MB
2	bajo	B
3	medio	M
4	alto	A
5	muy alto	MA

Fuente: (Ministerio de Administraciones Públicas, 2005)

3.10.5.2. Justificación de impactos para análisis de riesgos.

Para valorar el impacto en la matriz de riesgos se fijó el valor del impacto basado en la percepción de las actividades diarias que se realizan en la Dirección Nacional de Operaciones. También se apoyó en el criterio del señor Director que tiene muchos años de experiencia en el área y que trabaja día a día conjuntamente con los administradores de la dirección.

[17]Referencia: “Magerit versión 2 (Técnicas)”.

3.10.5.3. Calificación del impacto.

Como referencia se toma la pregunta 1 de la tabla 21 (disponibilidad del servicio), "¿Se monitorea la disponibilidad de los servicios en relación a la disponibilidad acordada?". Es decir el impacto que puede causar este indicador a los administradores de infraestructura por no realizar el monitoreo respectivo de la disponibilidad de los servicios considerados como críticos para el Ministerio de Finanzas, se lo considera con un valor de impacto "**alto"**.

El impacto en las labores diarias, si bien no es seguro que se den catástrofes todos los días (pero cuando ocurran consumirán demasiado tiempo y esfuerzo de los administradores de infraestructura) ha sido calificado con un valor igual a 4.

3.10.5.4. Amenazas.

Se relacionan con los indicadores que provienen de las preguntas realizadas a los administradores de infraestructura. Para generar una amenaza lo que se hace es colocar en forma negativa el indicador, esto quiere decir que se tendrá que transformar al indicador de tal manera que su ocurrencia de un resultado negativo.

Por ejemplo, para el ítem 2 de la tabla 21 (gestión de disponibilidad) donde se pronuncia: "¿Se monitorea la cantidad de interrupciones de servicio ocurridas?", fue transformado a negativo del indicador de: "Falta de monitoreo de la cantidad de interrupciones de servicio ocurridas".

Para los demás ítem correspondientes a la Gestión de Disponibilidad y de eventos se transformarán de la misma manera que en el ejemplo citado anteriormente.

3.10.5.5. Estimación del riesgo.

La fórmula para realizar el cálculo del riesgo relacionado a los procesos de disponibilidad y eventos, relacionados con ITIL V 3, se la ejecuta mediante la siguiente ecuación:

Riesgo = Impacto ***** Probabilidad de Amenaza

Dónde:

Impacto: Es la calificación que se proporciona a una amenaza identificada.

Para calcular la fórmula del riesgo se consultó del libro Magerit en su capítulo evaluación de riesgos relacionados con la tecnológica. (MHAP, 2012)

3.10.6. Análisis de riesgos.

A continuación se presentan las tablas con los resultados del análisis de riegos y sus respectivos impactos calificados a cada uno de los procesos relacionados con el marco de referencia ITIL V 3.

Esta matriz se conforma según los siguientes factores: amenaza, impacto, probabilidad de amenaza y el riesgo.

3.10.6.1. Gestión de Disponibilidad.

En la tabla siguiente se muestran cada una de las amenazas que podrían afectar a la gestión de disponibilidad.

Tabla 29

Resultados matriz de riesgos - Disponibilidad

N°	Amenaza	Impacto	Probabilidad de Amenaza	Riesgo
1	Falta de monitoreo de disponibilidad de los servicios en relación a la disponibilidad acordada.	4	0.66	2.64
2	Falta de monitoreo de la cantidad de interrupciones del servicio ocurridas.	4	0.33	1.32
3	Falta de existencia de monitoreo con respecto a la duración media de interrupciones de un servicio	4	0.33	1.32
4	Falta de monitoreo el porcentaje de servicios y componentes de infraestructura sujetos a monitorización de disponibilidad	2	1	2
5	Falta de conocimiento de la cantidad de medidas implementadas con el objetivo de aumentar la disponibilidad	4	1	4
			Promedio	**2.25**

Elaborado por: Wilman Sánchez

3.10.6.2. Gestión de Eventos.

A cada una de la 5 amenazas que podría afectar la continuidad del servicio se le asignó una calificación según su impacto, lo probabilidad que ocurra y el riesgo; los resultados se muestran en la siguiente tabla

Tabla 30

Resultados matriz de riesgos - eventos

N°	Amenaza	Impacto	Probabilidad de Amenaza	Riesgo
1	Falta monitoreo el número de eventos, por categorías	4	0.66	2.64
2	Carencia de un monitoreo del número de eventos, por importancia	4	0.66	2.64
3	Falta de monitoreo el número de eventos relacionados con problemas de rendimiento	4	0.66	2.64
4	Carencia de la existencia de monitoreo del número de eventos que indican futuros problemas de disponibilidad	4	0.66	2.64
5	Falta de monitoreo del tipo de evento, por aplicación	4	0.66	2.64
			Promedio	**2.64**

Elaborado por: Wilman Sánchez

3.10.7. Cálculo de riesgo promedio.

El promedio del valor de los riesgos por cada proceso evaluado se presente en la tabla siguiente.

Tabla 31

Resultados del riesgo promedio

PROCESO	RIESGO (Promedio)
Gestión de Disponibilidad	**2.25**
Gestión de Eventos	**2.64**

Elaborado por: Wilman Sánchez

3.10.7.1. Riesgos en disponibilidad.

Se aprecia un riesgo con calificación de tendencia **alta** para la gestión de disponibilidad. El ítem con mayor riesgo es debido a la falta de monitoreo y generación de reportes históricos de la disponibilidad de infraestructura, este factor hace que de una manera u otra la Dirección Nacional de Operaciones, desconozca la cantidad de medidas que pueden ser implementadas con el objetivo de aumentar la disponibilidad.

3.10.7.2. Riesgos en eventos.

El promedio de riesgo para la Gestión de Eventos que se realiza en la Dirección Nacional de Operaciones es igual a **2.64, lo cual equivale a una tendencia alta al riesgo**, es decir, la falta de monitoreo de eventos en la infraestructura hace que los administradores no puedan prever a tiempo futuras incidencias que ocurran en la infraestructura de los servicios eSigef y eSipren.

3.10.8. HP SITESCOPE versus Gestión de Disponibilidad y Eventos.

Es necesario en este punto realizar una comparación entre los indicadores que se toman en cuenta para la evaluación de la situación actual de la infraestructura de los aplicativos eSigef, eSipren y los indicadores que arrojan la herramienta de monitoreo con respecto a los servidores de infraestructura, de manera que se pueda capturar información que genera la HP SITESCOPE durante las tres últimas semanas.

En las tablas 32 y 33 se realiza la comparación entre los indicadores de los dos procesos más importantes tomados en cuenta en el desarrollo de este presente trabajo, como son la "Gestión de Disponibilidad" y la "Gestión de Eventos", los cuales se mencionan en las mejores prácticas de ITIL V3 y los indicadores relacionados con la herramienta HP SITESCOPE. Todos los valores descritos hacen referencia al anexo 2 donde se detalla la captura que se realiza mediante HP SITESCOPE.

Esta información fue capturada desde el lunes 3 de febrero del 2014 hasta el viernes 21 de febrero del 2014, durante los días laborables (lunes a viernes) en el Ministerio de Finanzas.

Proceso de Gestión de Disponibilidad versus HP SITESCOPE

Tabla 32

Indicadores de Gestión de Disponibilidad versus monitoreo

Procesos ITIL	**Indicadores con respecto a ITIL**	**Indicadores de HP SITESCOPE**	**Captura de información del 3 al 21 de febrero del 2014**		
			Semana 1	**Semana 2**	**Semana 3**
Gestión de Disponibilidad	Disponibilidad de servicios en relación a la disponibilidad acordada en los SLA's.	Disponibilidad de los servicios eSigef en relación al 99.9 % de la disponibilidad establecida	99.99 %	99.98 %	99.99 %
	Cantidad de interrupciones de servicio	Número de caídas de los servidores de la infraestructura de los servicios eSigef y eSipren	2 caídas	3 caídas	4 caídas
	Duración media de interrupciones de servicio	Duración media (average) de las caídas de los servidores de la infraestructura de los servicios eSigef y eSipren	5 min	5 min	5 min
	Porcentaje de servicios y componentes de infraestructura sujetos a monitorización de disponibilidad.	Número de servicios y componentes sujetos a monitorización de disponibilidad	14 componentes monitoreados para la infraestructura de los servicios eSigef y eSipren		
	Cantidad de medidas implementadas con el objetivo de aumentar la disponibilidad.	Reportes de monitoreo de recursos (CPU, memoria y disco) de los servidores de eSigef y eSipren	1 reporte	1 reporte	1 reporte

Proceso de Gestión de Eventos versus HP SITESCOPE

Tabla 33

Indicadores de Gestión de Eventos versus monitoreo

Procesos ITIL	**Indicadores con respecto a ITIL**	**Indicadores de HP SITESCOPE**	**Captura de información del 3 al 21 de febrero del 2014**		
			Semana 1	**Semana 2**	**Semana 3**
Gestión de Eventos	Número de eventos, por categorías.	Número de eventos por Aplicativo e Infraestructura monitoreados	3 eventos	2 eventos	5 eventos
	Número de eventos, por importancia.	Número de eventos de CPU, Memoria y Disco ocurridos.	5 eventos	2 eventos	5 eventos
	Número y porcentaje de eventos relacionados con problemas de rendimiento.	Número de eventos relacionados con alto consumo de la CPU y Memoria del eSigef y eSipren	6 eventos	5 eventos	5 eventos
	Número de eventos que indican futuros problemas de disponibilidad.	Número de eventos de aplicación (.NET) e infraestructura (CPU, Memoria, Disco) repetitivos para el eSigef eSipren	5 eventos	5 eventos	5 eventos
	Número de cada tipo de evento, por plataforma o aplicación.	Número de eventos ocurridos en la plataforma eSigef y eSipren	4 eventos	2 eventos	2 eventos

Proceso de Gestión de Eventos versus HP SITESCOPE

CAPÍTULO 4
PROPUESTA DE MONITOREO

En este capítulo se realiza la propuesta de monitoreo de la infraestructura de los servidores correspondiente a los sistemas eSigef y eSipren con apoyo de la herramienta HP SITESCOPE y el marco referencia de ITIL V3.

4.1. Antecedentes

En el capítulo 3 se realizó un análisis de riesgos que pueden afectar a la infraestructura de los servicios eSigef y eSipren donde se evidenció que el proceso de gestión de nivel de servicio no cumple con buenas prácticas del marco de referencia ITIL V3. Esto obedece a que no existe una adecuada planificación en el desarrollo de este proceso lo que permite que exista un riesgo a ser tomado en cuenta hacia la gestión de los servicios orientado al monitoreo. Debido a este antecedente se pretende desarrollar la propuesta de monitoreo siguiendo las recomendaciones de ITIL V3 que sirve como marco de referencia para mejorar este proceso crítico en la Dirección Nacional de Operaciones.

4.1.1. Niveles de riesgos según las encuestas.

En la tabla 34 se muestran los procesos de Gestión de Disponibilidad y eventos con su respectivo promedio de riesgo alcanzado. Se puede evidenciar que cada proceso relacionado con el marco de referencia ITIL V3, alcanzó el promedio de riesgo con un puntaje de 2.25 y 2.64 respectivamente, considerado por MAGERIT como riego alto.

Tabla 34

Riegos alcanzados por cada proceso

PROCESO	**RIESGO (Promedio)**
Gestión de Disponibilidad	**2.25**
Gestión de Eventos	**2.64**

Elaborado por: Wilman Sánchez

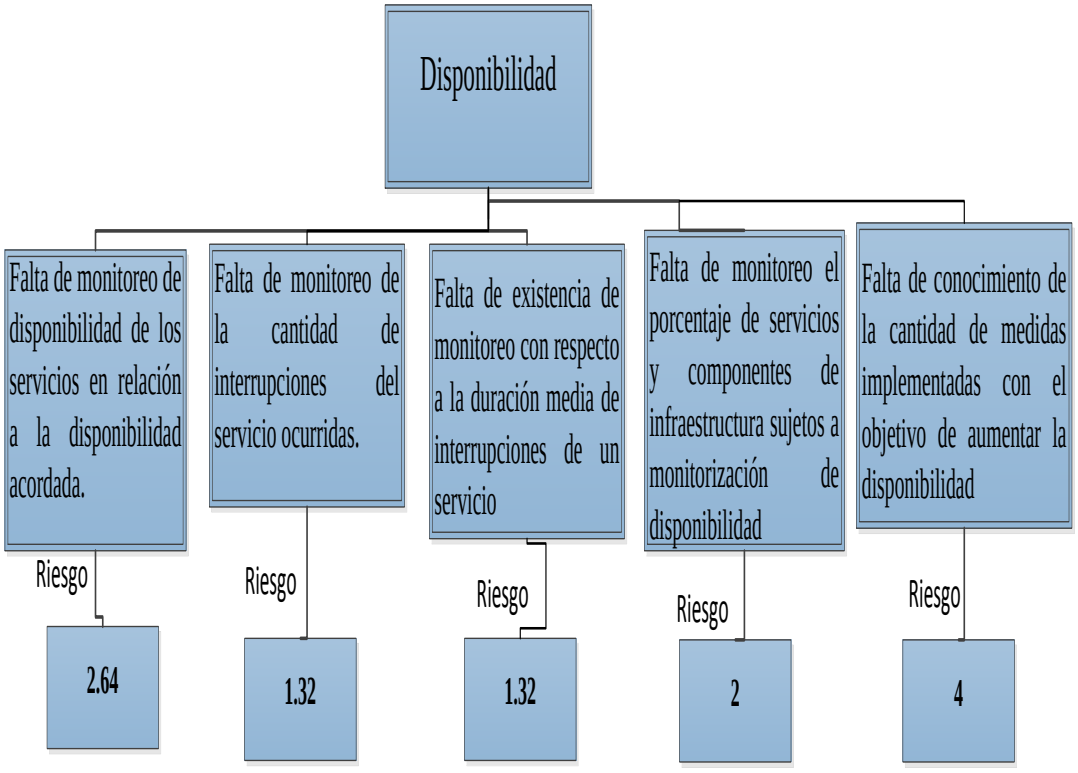
4.1.1.2. Estado actual de gestión del nivel de servicio.

De acuerdo al análisis de riesgos, los procesos de Gestión de Disponibilidad y de eventos analizados en el capítulo 3, deben ser tomados en cuenta ya que alcanzaron

promedios de riesgo igual a 2.25 y 2.64, respectivamente; siendo necesaria la intervención inmediata, porque según la Contraloría General del Estado todo valor superior a 2.0 implica una atención urgente.

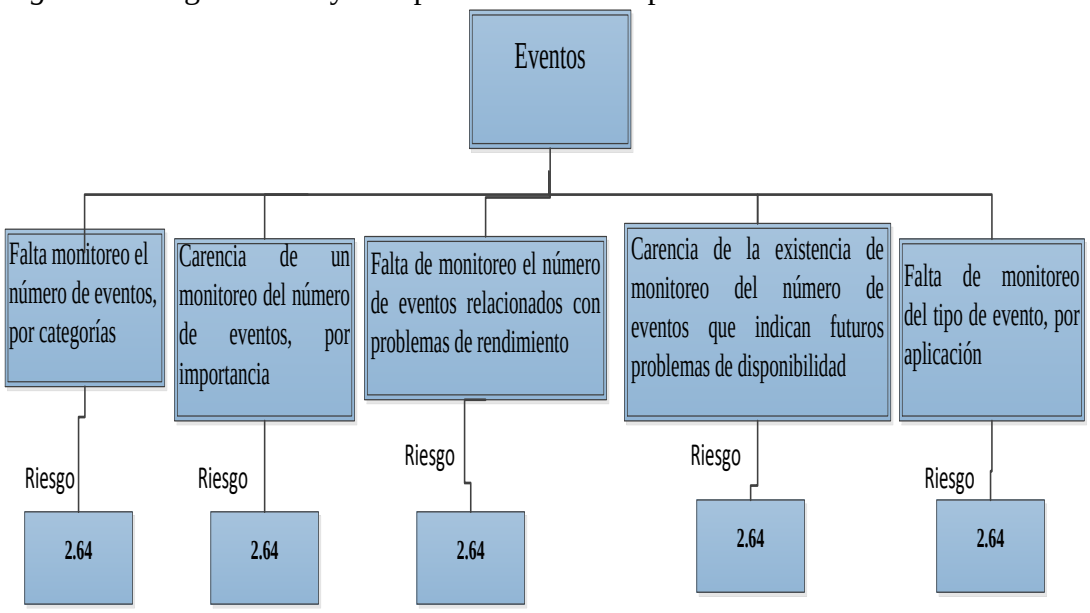
En la figura 17 y 18 se detallan los valores tomados a los administradores de la infraestructura con respecto a los procesos de disponibilidad y eventos.

Figura 17 Riegos con mayor importancia en la disponibilidad de servicios



Elaborado por: Wilman Sánchez

Figura 18 Riegos con mayor importancia en la disponibilidad de servicios



Elaborado por: Wilman Sánchez

4.2. Propuesta de monitoreo

Como monitoreo se conoce al conjunto de actividades ordenadas, priorizadas y automatizadas que validan, verifican y conocen el estado de un componente tecnológico o un servicio en tiempo real. Lo que permite tomar acciones preventivas o correctivas minimizando el impacto. (Cloud, 2010).

La propuesta de monitoreo se basa en actividades sugeridas por ITIL, tomando en cuenta los indicadores evaluados en la Dirección de Operaciones. El dominio de ITIL, manejo de disponibilidad de Servicio, se encuentra detallado en el libro de diseño donde se establece que la planificación debe asegurar la continuidad de los servicios por parte del proveedor para que los usuarios puedan cumplir con sus funciones.

Partiendo del marco teórico descrito del capítulo 2 y basándose en el análisis realizado en el capítulo 3, se pretende dar lineamientos claros a fin de proponer un mecanismo y/o proceso que permita mejorar el monitoreo de disponibilidad de infraestructura. Además de realizar el seguimiento a los incidentes y problemas mediante un procedimiento de monitoreo.

4.2.1. Actividades a realizarse.

En referencia a las buenas prácticas de ITIL V3, se realiza la propuesta enfocada a la infraestructura tecnológica y su gestión. Además está orientada a dar seguimiento del funcionamiento, comportamiento de los recursos de hardware y software de los servidores, con ayuda de HP SITESCOPE como herramienta de monitoreo de infraestructura.

En base al análisis de gestión de riesgos y las mejores prácticas de ITIL se debe asignar responsables del monitoreo para la Dirección Nacional de Operaciones con el objetivo de contar con el personal adecuado para realizar el proceso de monitoreo, se plantea realizar:

- Responsables de la Gestión de Disponibilidad y Eventos.
- Notificación y seguimiento de incidencias ocurridas en infraestructura.
- Notificación y seguimiento de problemas ocurridos en infraestructura.

4.2.2. Plan de acción.

Los responsables de la Gestión de Disponibilidad y Eventos, tienen como objetivo primordial conocer de manera rápida cualquier incidente o problema que cause interrupción en la infraestructura de los servidores correspondiente a los servicios eSigef y eSipren, mediante notificaciones e informes de monitoreo presentados a los analistas de infraestructura correspondientes.

El afinamiento de umbrales en la herramienta de monitoreo es necesario como medida de mejora y de acuerdo a las mejores prácticas descritas por los fabricantes de infraestructura tecnológica de apoyo a una correcta monitorización de aplicaciones .Net, recursos de hardware de los servidores y red. Por esta razón se propone mejorar sustancialmente la configuración de la herramienta HP SITESCOPE enfocada a la monitorización de los servicios, sin embargo no todas las configuraciones de umbrales son aplicadas a la realidad del Ministerio de Finanzas, razón por la cual se dará seguimiento a los siguientes aspectos:

- Definir las actividades a realizarse para los responsables del monitoreo.

- Mantener la configuración de HP SITESCOPE de acuerdo a la realidad variable que posee la infraestructura de la Dirección de Operaciones.
- Notificación de incidencias ocurridas en infraestructura.
- Notificación de problemas ocurridos en infraestructura.

4.2.2.1. Responsables de la Gestión de Disponibilidad y Eventos.

Para establecer un servicio de monitoreo de alto nivel apoyado de la Gestión de Disponibilidad y de eventos, se propone realizar la implementación de un procedimiento de notificación de incidencias y problemas. Además se deberá establecer la configuración de umbrales en HP SITESCOPE correspondiente a la criticidad de cada monitor establecido en esta herramienta

La utilización de HP SITESCOPE administra todos los eventos, incidentes y problemas primordiales de un servicio de monitoreo de infraestructura. Es decir, permite adelantarse a cualquier eventualidad que pueda ocurrir en la disponibilidad de los servicios y/o resolver los problemas en el menor tiempo posible. Además la recolección de información para la elaboración de informes se basará en alertas que ocurran en la infraestructura tecnológica del centro de datos del Ministerio de Finanzas.

4.2.2.2. Gestión de Incidencias.

Tiene como objetivo encontrar y analizar de la manera más rápida posible cualquier alteración que cause una interrupción en el servicio.

> La gestión de incidencias no debe confundirse con la gestión de problemas, pues a diferencia de esta última, no se preocupa de encontrar y analizar las causas subyacentes a un determinado incidente sino exclusivamente a restaurar el servicio. Sin embargo, es obvio, que existe una fuerte interrelación entre ambas. (Osiatis, 2011).

4.2.2.3. Funciones.

Se establecen funciones sobre el personal responsable del monitoreo con el propósito de monitorear la disponibilidad, eventos, incidentes y problemas. Además de identificar amenazas presentadas en los equipos de infraestructura a monitorear. En este caso la responsabilidad de entrega de información está dirigida por un líder.

Los incidentes presentados en infraestructura se deben priorizar según el impacto del servidor monitoreado y los servicios que esté prestando. Estas prioridades podrían clasificarse como: **alta, media, baja.**

4.2.2.4. Asignación de recursos.

Para un monitoreo eficiente de infraestructura se requiere como recursos principales el personal responsable de monitoreo y de la herramienta HP SITESCOPE; la utilización de esta herramienta de monitoreo se debe a que fue adquirida con la infraestructura de servidores en el año 2012, la misma que no es utilizada de la mejor manera, además actualmente no se cuenta con personal calificado para la administración de este recurso.

4.2.2.4.1. Personal requerido para la Gestión de Eventos y Disponibilidad.

Según el director de la Dirección Nacional de Operaciones, el perfil de las personas responsables del monitoreo deben cumplir con los siguientes requisitos:

1. Poseer Titulo de 3er. Nivel en Ingeniería de Sistemas.
2. Experiencia en herramientas de monitoreo similares a HP SITESCOPE de al menos un año.
3. Poseer cursos de capacitación en herramientas de monitoreo.

El número tentativo de personas responsables del monitoreo, se dará de acuerdo a la dimensión de la infraestructura, es de 3 personas incluyendo el líder del área.

4.2.2.4.2. Herramienta HP SITESCOPE.

Los requerimientos mínimos para la utilización de la herramienta de monitoreo son:

- Actualización a la última versión.
- Instalación de parches de seguridad

Es necesario realizar la renovación del licenciamiento de la herramienta para obtener las ventajas con el fabricante, así como nuevas versiones, acceso a material de apoyo relacionado con el monitoreo de infraestructura y soporte técnico bajo la siguiente modalidad.

Tabla 35

Modalidad de soporte técnico

Modalidad	Descripción
9x5	Nueve (9) horas al día y cinco (5) días a la semana. El horario de soporte de monitoreo sería de 9:00h a 18:00h ininterrumpidamente.

Elaborado por: Wilman Sánchez

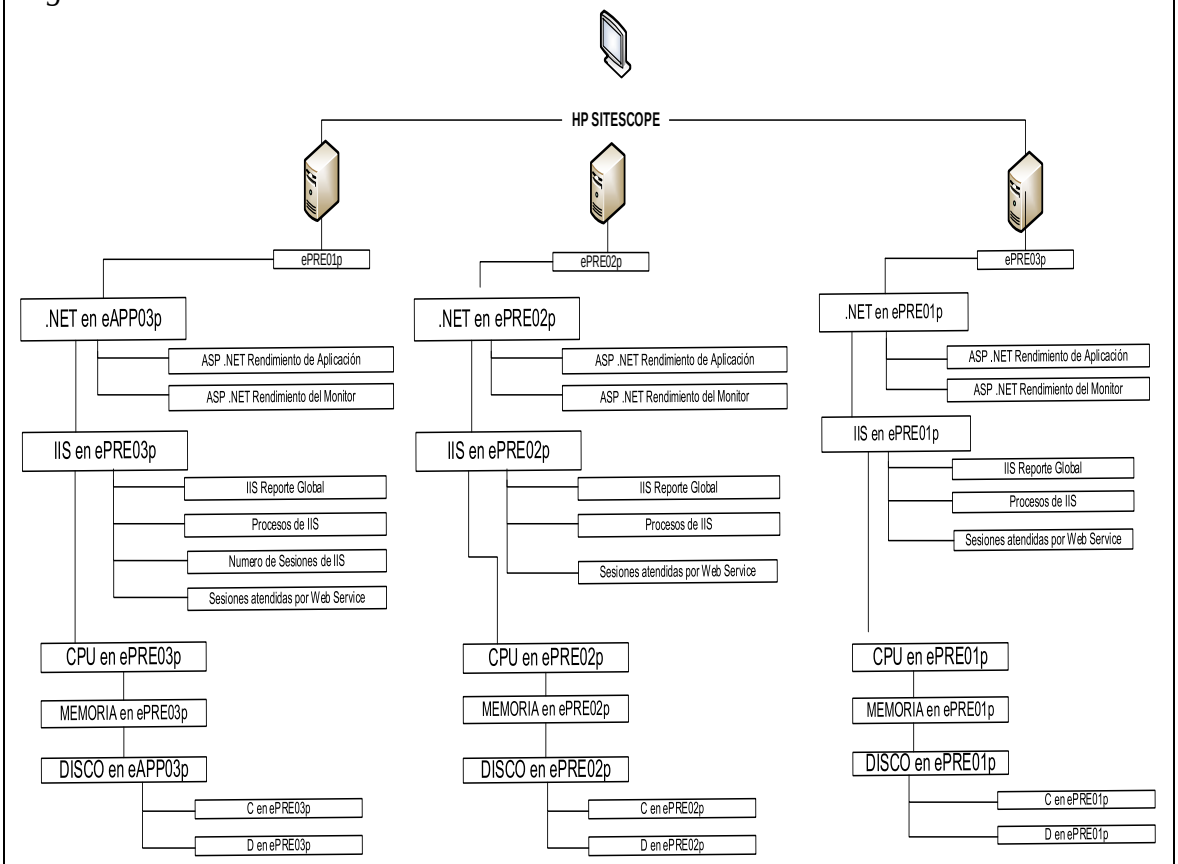
La ventaja en el uso de esta herramienta de monitoreo se lo presenta en el punto 2.6 del trabajo de titulación. Es necesario tomar en consideración que esta herramienta por el hecho de ser comercial cuenta con soporte técnico en la modalidad que se describe en la tabla 33, debido a esto se cuenta con un respaldo a cualquier inconveniente presentado en su uso.

4.2.2.5. Diagrama de infraestructura de los servicios.

A continuación se muestran los componentes de la infraestructura por cada servicio a ser monitoreado. El diagrama ayudará al personal de monitoreo a tener en cuenta cada uno de los componentes que necesitan ser monitoreados por la herramienta de HP SITESCOPE.

4.2.2.5.1. Infraestructura de monitoreo de los servicios

Figura 19 Infraestructura a ser monitoreada



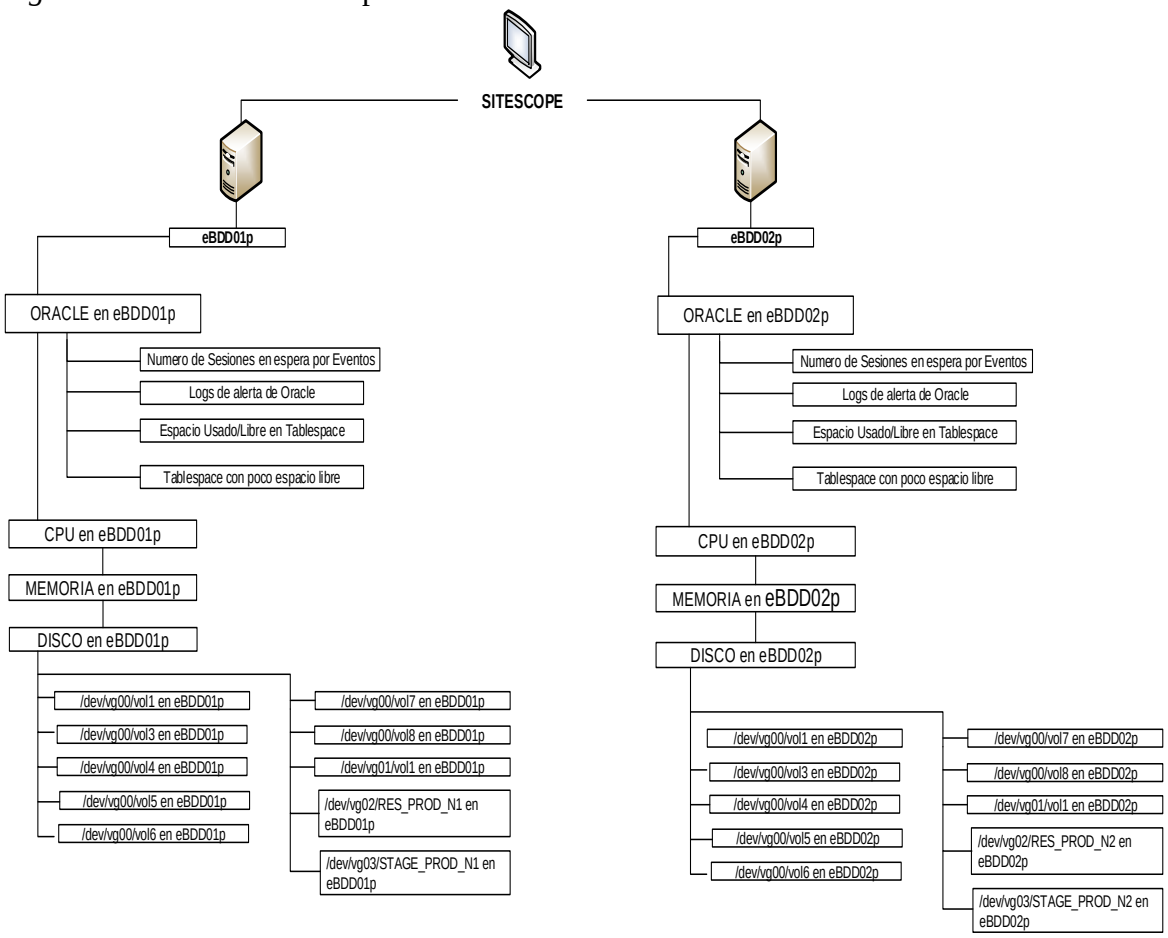
Elaborado por: Wilman Sánchez

La figura 19 muestra los componentes principales de infraestructura correspondiente a los servicios a ser monitoreados, estos son:

- .**NET:** Archivos dll que ayudan a ejecutar la aplicación.
- **IIS:** Servidor web del aplicativo eSigef
  - IIS reporte global.
  - Procesos de IIS.
  - Número de sesiones de IIS.
  - Sesiones atendidas por IIS.
- **CPU:** Unidad de procesamiento central del servidor.
- **Memoria**: Memoria de acceso aleatorio.
- **Disco:** Unidad de almacenamiento local pertenecientes al servidor donde se alojan los archivos de configuración.

4.2.2.5.2. Infraestructura de la capa base de datos.

Figura 20 Infraestructura capa base de datos - ORACLE



Elaborado por: Wilman Sánchez

La figura 20, muestra los componentes principales a ser monitoreados para la capa de base de datos, estos son:

- **Oracle:** Número de sesiones que están llegando a la base de datos desde aplicación y logs de alerta que se encuentran en los servidores con sistema operativo HP-UX.
  - Número de sesiones en espera por eventos.
  - Logs de alerta de Oracle.
  - Espacio usado/libre en tablespaces.
  - Tablespaces con poco espacio libre.
- **CPU:** unidad de procesamiento central del servidor
- **Memoria**: memoria de acceso aleatorio.

- **Disco:** conformado por tablespaces[18], que se encuentran dentro del servidor de base de datos Oracle.

4.2.2.6. Servidores y recursos a ingresar al monitoreo.

4.2.2.6.1. Servidores de infraestructura.

De acuerdo a la criticidad del servicio, los servidores y recursos a ser tomados en cuenta para el monitoreo están descritos en la tabla 36.

Tabla 36

Servidores y recursos

Servidores de infraestructura - eSigef		
Capas	**Servidor**	**Componentes**
Presentación	ePRE01p	Procesador. Memoria de acceso aleatorio. Almacenamiento.
	ePRE02p	
	ePRE03p	
Aplicación	eAPP01p	
	eAPP02p	
	eAPP03p	

Elaborado por: Wilman Sánchez

4.2.2.6.2. Servidores de infraestructura.

De acuerdo a la criticidad del servicio eSipren, los servidores y recursos a ser tomados en cuenta para el monitoreo están descritos en la tabla 37.

Tabla 37

Componentes de infraestructura

Servidores de Infraestructura - eSipren		
Capas	**Servidor**	**Componentes**
Presentación	ePRE60p	Procesador Memoria de acceso aleatorio Almacenamiento
	ePRE61p	
Aplicación	eAPP60p	
	eAPP61p	

Elaborado por: Wilman Sánchez

[18] Unidad de almacenamiento lógico

4.2.2.6.3. Servidores de base de datos.

Los servidores y recursos a ser tomados en cuenta para el monitoreo de la capa base de datos se presentan en la tabla 38.

Tabla 38

Componentes de base de datos

Servidores de Base de Datos		
Capas	**Servidor**	**Componentes**
Base de Datos	eBDD01p	Procesador. Memoria de Acceso aleatorio. Tablespaces.[19]
	eBDD02p	

Elaborado por: Wilman Sánchez

4.2.2.7. Actividades del personal encargado.

Las actividades más importantes que debe cumplir por el personal responsable del monitoreo es:

- Definición de monitores en HP SITESCOPE
- Afinamiento de umbrales en HP SITESCOPE.
- Procedimiento de monitoreo a considerar.
- Informes de monitoreo.

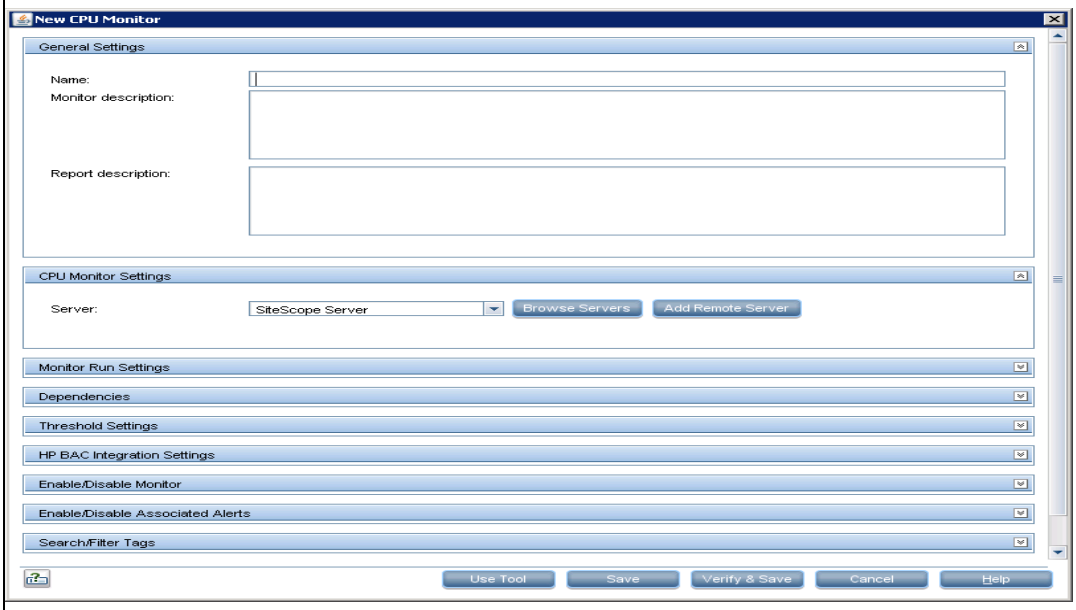
4.2.2.8. Definición de monitores en HP SITESCOPE.

Los tipos de monitores que tiene HP SITESCOPE, los cuales se utilizarán para el monitoreo de la infraestructura tecnológica serán:

Monitor de CPU: Este monitor presenta el rendimiento y disponibilidad de la CPU correspondiente al servidor configurado en la herramienta de monitoreo HP SITESCOPE. En la figura 21 se presentan los datos necesarios para ingresar un monitor de CPU y en la figura 22 se presenta un resumen de los recursos que están siendo monitoreados.

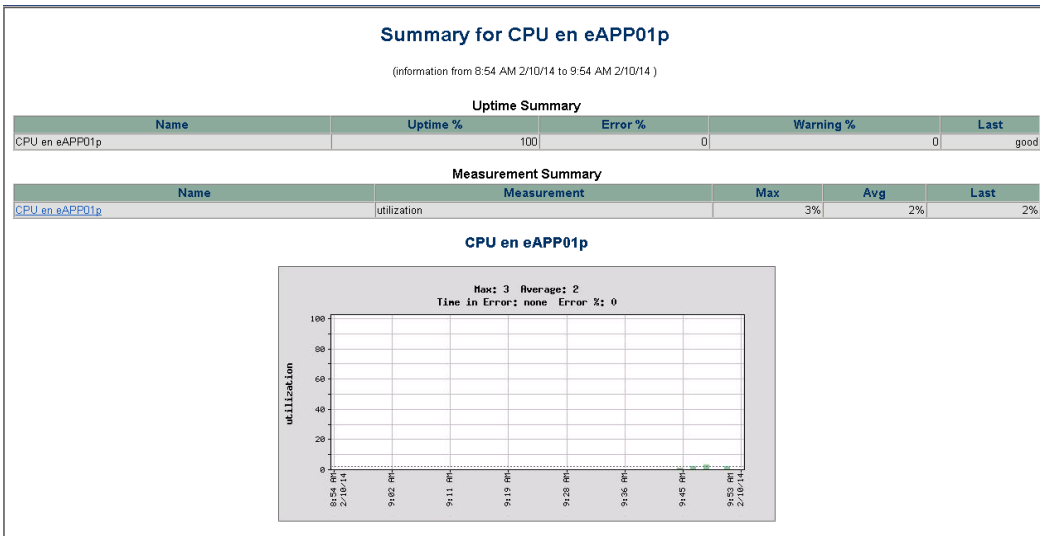
[19] **Tablespace:** Unidad lógica de almacenamiento

Figura 21 Monitor de CPU



Fuente: Ministerio de Finanzas, 2014**.**

Figura 22 Resumen del recurso CPU

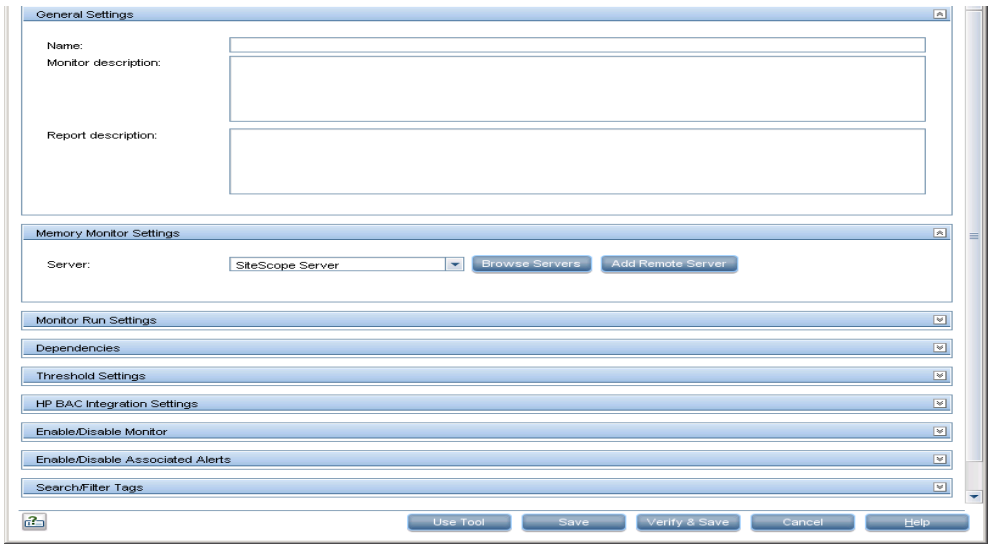


Fuente: Ministerio de Finanzas, 2014.

Monitor de utilización de la memoria: Este monitor presenta el rendimiento y disponibilidad de la memoria de acceso aleatorio correspondiente al servidor configurado en la herramienta de monitoreo HP SITESCOPE. En la figura 23 se

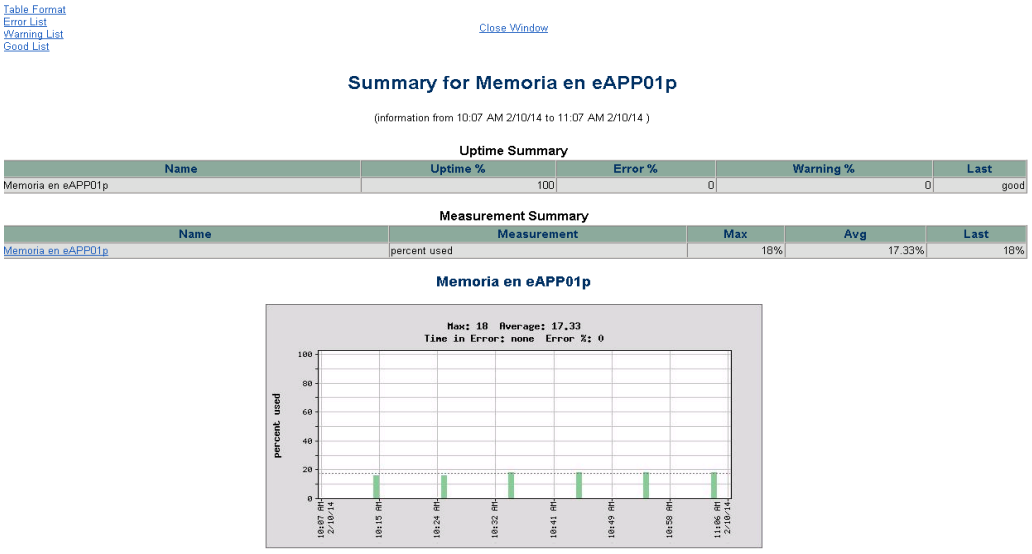
presentan los datos necesarios para ingresar un monitor de memoria y en la figura 24 se presenta un resumen de los recursos que están siendo monitoreados.

Figura 23 Monitor de memoria



Fuente: Ministerio de Finanzas, 2014.

Figura 24 Resumen del recurso memoria

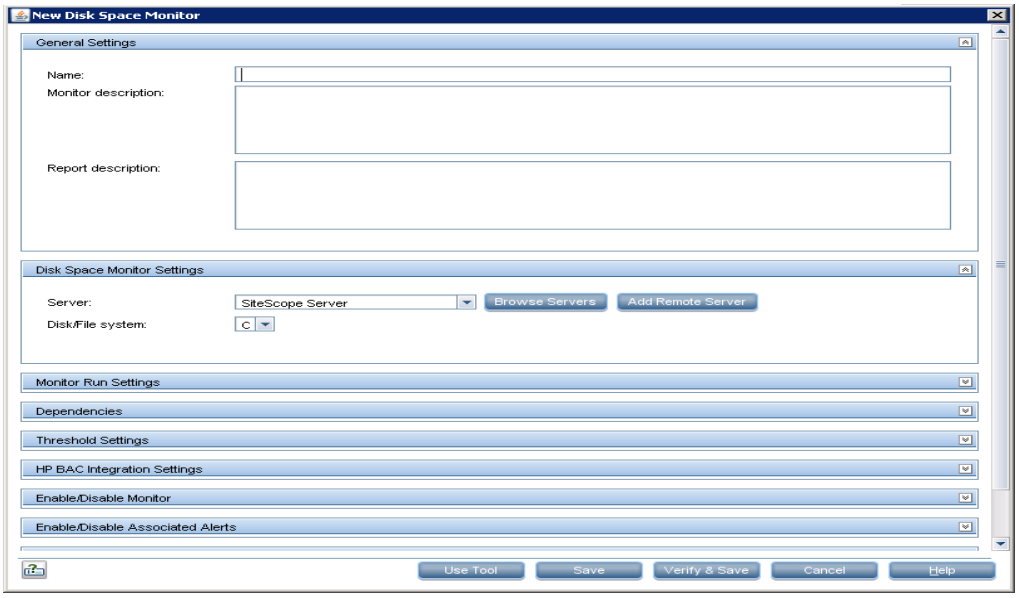


Fuente: Ministerio de Finanzas, 2014.

Monitor de espacio en disco: Este monitor presenta la disponibilidad y el porcentaje de espacio usado en discos locales de los servidores configurados en HP SITESCOPE. En

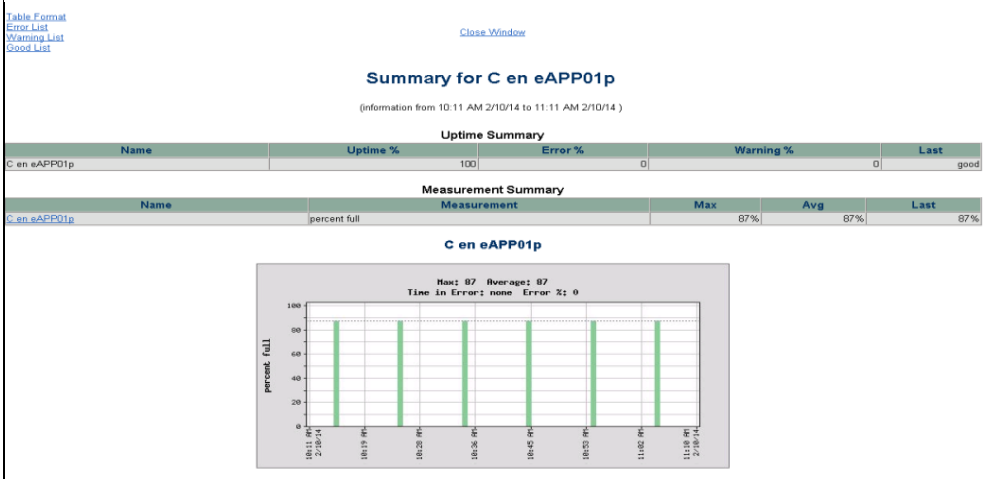
la figura 25 se presentan los datos necesarios para ingresar un monitor de disco y en la figura 26, se presenta un resumen de los recursos que están siendo monitoreados.

Figura 25 Monitor de espacio en disco



Fuente: Ministerio de Finanzas, 2014.

Figura 26 Resumen de espacio en disco

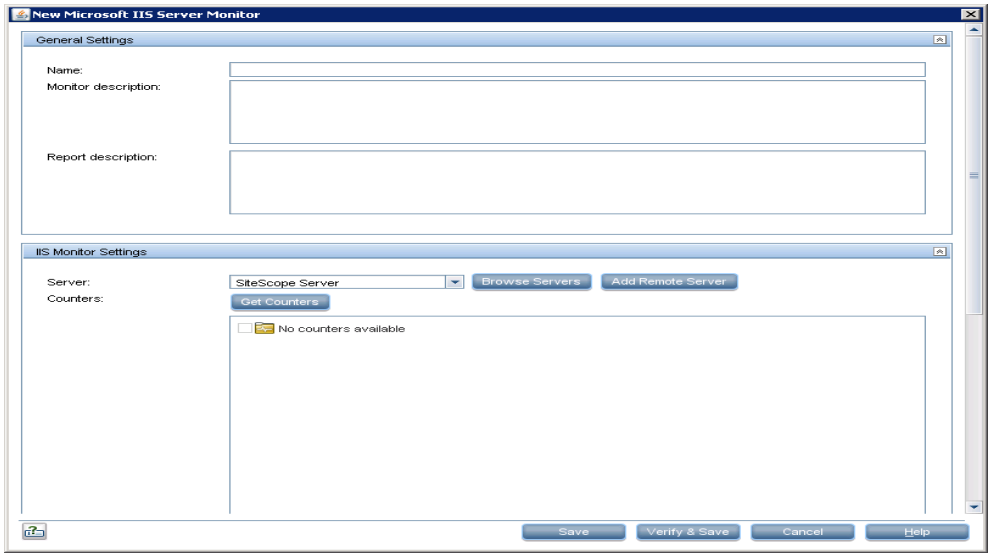


Fuente: Ministerio de Finanzas, 2014.

Monitor de Servidor IIS de Microsoft: Este monitor presenta el rendimiento y disponibilidad del servidor de IIS de Microsoft correspondiente al servidor configurado en la herramienta de monitoreo HP SITESCOPE. En la figura 27 se presentan los datos

necesarios para ingresar un monitor de IIS de Microsoft y en la figura 28 se presenta un resumen de los recursos que están siendo monitoreados.

Figura 27 Monitor de Servidor IIS (Internet Information Service)



Fuente: Otorgado por Ministerio de Finanzas

Figura 28 Resumen del recurso IIS (Internet Information Service)

Table Format
Error List
Warning List
Good List

Close Window

Summary for Multiple Monitors

(information from 10:17 AM 2/10/14 to 11:17 AM 2/10/14)

Uptime Summary

Name	Uptime %	Error %	Warning %	Last
IS Server en eAPP01p	100	0	0	good
IS Process en eAPP01p	0	100	0	ERROR
IS Global en eAPP01p	100	0	0	good
MSMQ Queue en eAPP01p	100	0	0	good
Web Service en eAPP01p	100	0	0	good
ndexing Service en eAPP01p	100	0	0	good
Numero de Sesiones	100	0	0	good

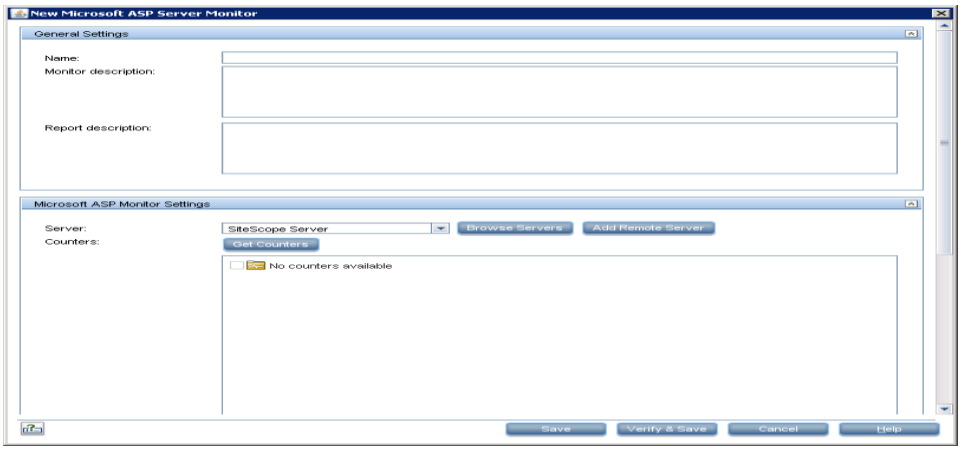
Measurement Summary

Name	Measurement	Max	Avg	Last
IS Server en eAPP01p	Server : Bytes Transmitted/sec:SINGLE	0	0	0
IS Process en eAPP01p	counters in error	0	0	0
IS Process en eAPP01p	Process\inetinfo\Working Set	25178112	25164458	25161728
IS Process en eAPP01p	Process\inetinfo\Page Faults/sec	0.01	0	0
IS Process en eAPP01p	Process\inetinfo\% Processor Time	0.01	0	0
IS Process en eAPP01p	Process\inetinfo\Thread Count	11	10.17	10
IS Process en eAPP01p	Process\inetinfo\Private Bytes	18178048	18137088	18128896
IS Global en eAPP01p	Internet Information Services Global : File Cache Hits %:SINGLE	n/a	n/a	n/a
MSMQ Queue en eAPP01p	Server : Bytes Transmitted/sec:SINGLE	0	0	0
Web Service en eAPP01p	Web Service : Bytes Total/sec:esigef.mef.gov.ec	n/a	n/a	n/a
Web Service en eAPP01p	Web Service : Current Blocked Async I/O Requests:esigef.mef.gov.ec	n/a	n/a	n/a
Web Service en eAPP01p	Web Service : Current Connections:esigef.mef.gov.ec	n/a	n/a	n/a
Web Service en eAPP01p	Web Service : Files/sec:esigef.mef.gov.ec	n/a	n/a	n/a
Web Service en eAPP01p	Web Service : Get Requests/sec:esigef.mef.gov.ec	n/a	n/a	n/a
Web Service en eAPP01p	Web Service : Measured Async I/O Bandwidth Usage:esigef.mef.gov.ec	n/a	n/a	n/a
Web Service en eAPP01p	Web Service : Not Found Errors/sec:esigef.mef.gov.ec	n/a	n/a	n/a
ndexing Service en eAPP01p	Server : Bytes Transmitted/sec:SINGLE	0	0	0
Numero de Sesiones	Server : Server Sessions:SINGLE	4	3.67	4

Fuente: Ministerio de Finanzas, 2014.

Monitor de Microsoft ASP[20]: Este monitor presenta el rendimiento y disponibilidad del servidor de ASP de Microsoft correspondiente al servidor configurado en la herramienta de monitoreo HP SITESCOPE. En la figura 29 se presentan los datos necesarios para ingresar un monitor de ASP de Microsoft y en la figura 30 se presenta un resumen de los recursos que están siendo monitoreados.

Figura 29 Monitor de ASP



Fuente: Ministerio de Finanzas, 2014.

Figura 30 Resumen del recurso ASP

Table Format
Error List
Warning List
Good List

Close Window

Summary for Multiple Monitors

(information from 10:20 AM 2/10/14 to 11:20 AM 2/10/14)

Uptime Summary

Name	Uptime %	Error %	Warning %	Last
ASP.NET Applications Performance monitor en eAPP02p	0	0	0	DISABLED
ASP.NET Performance monitor en eAPP02p	0	0	0	DISABLED

Measurement Summary

Name	Measurement	Max	Avg	Last
ASP.NET Applications Performance monitor en eAPP02p	counters in error	n/a	n/a	17
ASP.NET Applications Performance monitor en eAPP02p	ASP.NET Apps v2.0.50727__Total__\Requests Executing	n/a	n/a	n/a
ASP.NET Applications Performance monitor en eAPP02p	ASP.NET Apps v2.0.50727__Total__\Pipeline Instance Count	n/a	n/a	n/a
ASP.NET Applications Performance monitor en eAPP02p	ASP.NET Apps v2.0.50727__Total__\Output Cache Turnover Rate	n/a	n/a	n/a
ASP.NET Applications Performance monitor en eAPP02p	ASP.NET Apps v2.0.50727__Total__\Compilations Total	n/a	n/a	n/a
ASP.NET Applications Performance monitor en eAPP02p	ASP.NET Apps v2.0.50727__Total__\Cache Total Entries	n/a	n/a	n/a
ASP.NET Applications Performance monitor en eAPP02p	ASP.NET Apps v2.0.50727__Total__\Output Cache Entries	n/a	n/a	n/a
ASP.NET Applications Performance monitor en eAPP02p	ASP.NET Apps v2.0.50727__Total__\Cache API Turnover Rate	n/a	n/a	n/a
ASP.NET Applications Performance monitor en eAPP02p	ASP.NET Apps v2.0.50727__Total__\Errors During Preprocessing	n/a	n/a	n/a
ASP.NET Applications Performance monitor en eAPP02p	ASP.NET Apps v2.0.50727__Total__\Cache API Entries	n/a	n/a	n/a
ASP.NET Applications Performance monitor en eAPP02p	ASP.NET Apps v2.0.50727__Total__\Cache API Hit Ratio	n/a	n/a	n/a
ASP.NET Applications Performance monitor en eAPP02p	ASP.NET Apps v2.0.50727__Total__\Sessions Active	n/a	n/a	n/a
ASP.NET Applications Performance monitor en eAPP02p	ASP.NET Apps v2.0.50727__Total__\Cache Total Turnover Rate	n/a	n/a	n/a
ASP.NET Applications Performance monitor en eAPP02p	ASP.NET Apps v2.0.50727__Total__\Errors Total	n/a	n/a	n/a
ASP.NET Applications Performance monitor en eAPP02p	ASP.NET Apps v2.0.50727__Total__\Sessions Total	n/a	n/a	n/a
ASP.NET Applications Performance monitor en eAPP02p	ASP.NET Apps v2.0.50727__Total__\Cache Total Hit Ratio	n/a	n/a	n/a
ASP.NET Applications Performance monitor en eAPP02p	ASP.NET Apps v2.0.50727__Total__\Output Cache Hit Ratio	n/a	n/a	n/a
ASP.NET Applications Performance monitor en eAPP02p	ASP.NET Apps v2.0.50727__Total__\Requests In Application Queue	n/a	n/a	n/a
ASP.NET Performance monitor en eAPP02p	counters in error	n/a	n/a	10
ASP.NET Performance monitor en eAPP02p	ASP.NET v2.0.50727\Application Restarts	n/a	n/a	n/a
ASP.NET Performance monitor en eAPP02p	ASP.NET v2.0.50727\State Server Sessions Total	n/a	n/a	n/a
ASP.NET Performance monitor en eAPP02p	ASP.NET v2.0.50727\Requests Current	n/a	n/a	n/a
ASP.NET Performance monitor en eAPP02p	ASP.NET v2.0.50727\Request Execution Time	n/a	n/a	n/a
ASP.NET Performance monitor en eAPP02p	ASP.NET v2.0.50727\State Server Sessions Active	n/a	n/a	n/a
ASP.NET Performance monitor en eAPP02p	ASP.NET v2.0.50727\Request Wait Time	n/a	n/a	n/a
ASP.NET Performance monitor en eAPP02p	ASP.NET v2.0.50727\Applications Running	n/a	n/a	n/a
ASP.NET Performance monitor en eAPP02p	ASP.NET v2.0.50727\Worker Process Restarts	n/a	n/a	n/a
ASP.NET Performance monitor en eAPP02p	ASP.NET v2.0.50727\Requests Queued	n/a	n/a	n/a
ASP.NET Performance monitor en eAPP02p	ASP.NET v2.0.50727\Worker Processes Running	n/a	n/a	n/a

Fuente: Ministerio de Finanzas, 2014.

[20] ASP: Application Service Providers

4.2.2.8.1. Afinamiento de umbrales en HP SITESCOPE.

En el anexo 3, se describe la configuración de umbrales para los servidores correspondientes al monitoreo los servicios eSigef y eSipren acorde a las mejores prácticas descritas por los fabricantes de infraestructura, donde se definen los valores de cada monitor que sean necesarios para la configuración de la herramienta HP SITESCOPE.

4.2.2.8.2. Afinamiento de umbrales en los servidores.

En la tabla 39 se presentan los umbrales a configurar en la infraestructura de los servidores y en la tabla 40 se presentan los umbrales a configurar en los servidores de base datos.

Tabla 39

Parámetros de umbrales a establecer en los servidores

Servidores	Ítems de configuración		Métricas	Descripción	Umbrales a establecer		
ePRE01p ePRE02p ePRE03p eAPP01p eAPP02p eAPP03p	CPU		% de Utilización	Utilización de la CPU media, en porcentaje (el valor promedio entre todas las CPU presentes en el sistema).	**GOOD < 90%**	**WARNING >= 90%**	**ERROR = 100%**
	MEMORIA		% de Utilización	Nivel total del uso de la memoria	**GOOD < 90%**	**WARNING > 80%**	**ERROR > 90 %**
	DISCO C:		% de Utilización	Cantidad relativa de espacio utilizado en la unidad donde está montado el sistema operativo.	**GOOD < 90%**	**WARNING >= 90%**	**ERROR >= 95%**
	DISCO D:		% de Utilización	Cantidad relativa de espacio libre en el disco secundario D:	**GOOD > 10 %**	**WARNING <= 10%**	**ERROR <= 5%**
	PING		% de Paquetes Buenos	Medir los paquetes de disponibilidad del host monitoreado.	**GOOD = 100%**	**WARNING < 100%**	**ERROR = 0%**
	IIS	Procesos del Monitor IIS	Working Set / Trabajo Conjunto	Muestra el número actual en bytes del conjunto de trabajo de este proceso. El conjunto de trabajo es el conjunto de páginas de memoria que se utilizaron recientemente por los subprocesos del proceso.	**GOOD < 15000000 bytes**	**WARNING >= 15000000 bytes**	**ERROR >= 20000000 bytes**
		Monitor del servidor	Bytes Transmitidos	Muestra la velocidad a la que el servidor envía bytes de datos a la red. Este contador indica la carga del servidor.	**GOOD < 64000 bytes/seg.**	**WARNING >= 64000 bytes/seg.**	**ERROR >= 90000 bytes/seg.**
		Monitor del Servicio Web	Bytes Totales	La suma de la tasa total en segundos, en el que los bytes de datos se han enviado y recibido por el servicio WWW.	**GOOD < 48000 bytes**	**WARNING >= 48000 bytes**	**ERROR >=64000 bytes**
	.NET	Disponibilidad en .NET	Estado: up/down	Monitoreo la Disponibilidad .NET	**GOOD UP**	**NA**	**ERROR DOWN**

Elaborado por: Wilman Sánchez

Tabla 40

Parámetros de umbrales a establecer en los servidores de base de datos

SERVIDOR	CI (ítems de Configuración)		METRICAS	DESCRIPCION	UMBRALES A ESTABLECER		
eBDD01p eBDD02p	CPU[21]		% de Utilización	Utilización de la CPU media, en porcentaje (el valor promedio entre todas las CPU presentes en el sistema).	**GOOD < 90%**	**WARNING >= 90%**	**ERROR >= 95%**
						WARNING >= 90%	**ERROR >= 95%**
	MEMORIA		% de Utilización	Nivel total del uso de la memoria.	**GOOD < 90%**	**WARNING =1**	**ERROR =0**
	PING[22]		% de Paquetes Buenos	Medir los paquetes de disponibilidad del servidor monitoreado.	**GOOD = 100%**		
	TABLESPACE	/dev/vg00/vol1	% de Utilización	Cantidad relativa de espacio utilizado en la unidad donde está montado el sistema operativo del nodo 1.	**GOOD < 90%**		
		/dev/vg00/vol3	% de Utilización	Espacio de Tablespace usado.	**GOOD < 90%**		
		/dev/vg00/vol4	% de Utilización	Espacio de Tablespace usado.	**GOOD < 90%**		
		/dev/vg00/vol5	% de Utilización	Espacio de Tablespace usado	**GOOD < 90%**		
		/dev/vg00/vol6	% de Utilización	Espacio de Tablespace usado	**GOOD < 90%**		
		/dev/vg02/RES_PROD_N1	% de Utilización	Espacio de Tablespace usado para respaldos del Nodo 1	**GOOD < 90%**		
		/dev/vg03/STAGE_PROD_N1	% de Utilización	Espacio de Tablespace usado para respaldos del Nodo 1	**GOOD < 90%**		
	ORACLE	Instancia ORACLE (prod)	Número de Instancias	Número de Instancias Disponibles en Oracle JDBC	**GOOD >1**		

Elaborado por: Wilman Sánchez

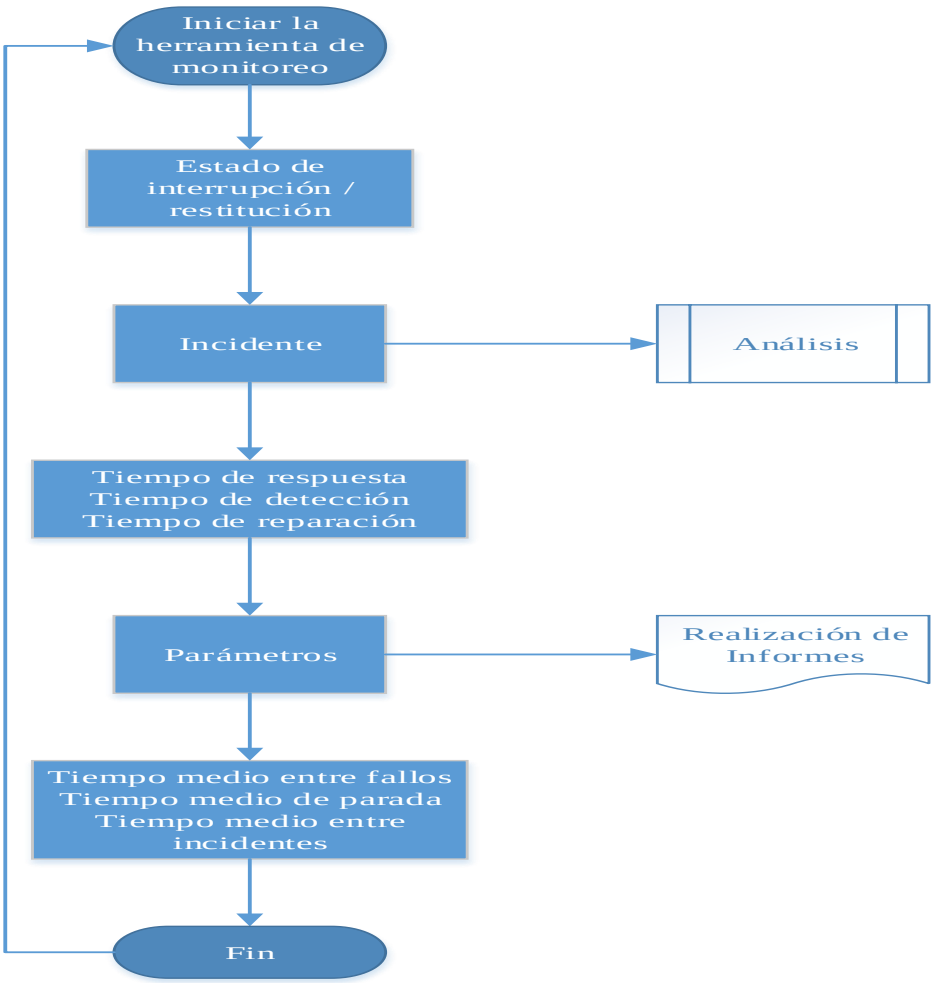
[21] CPU: Unidad central de procesamiento

[22] PING: Rastreador de paquetes en redes

4.2.2.9. Procedimiento de monitoreo a considerar.

A continuación se describe el procedimiento a tomar en cuenta por el personal responsable del monitoreo de los servidores correspondientes a la infraestructura de los servicios eSigef y eSipren. Este procedimiento se encuentra accesible a cambios.

Figura 31 Procedimiento de monitoreo



Elaborado por: Wilman Sánchez

4.2.2.9.1. Descripción procedimiento general.

El procedimiento de monitoreo inicia cuando se ejecuta la herramienta de monitoreo HP SITESCOPE que está instalada como parte de la infraestructura, luego que el administrador de monitoreo haya ejecutado este servicio, existen 2 estados en los que pueden permanecer los servidores de infraestructura, puede ser de interrupción o restitución. A continuación se analizará el incidente ocurrido de acuerdo al estado en que

se encuentra, a este tipo de incidente se aplicará los parámetros de tiempo de **respuesta, detección o reparación**.

La parte primordial del monitoreo está en el detalle de todos los parámetros a considerar en los informes, entre estos tiempos se tiene: **tiempo medio entre fallos, paradas y entre incidentes**; una vez cumplido los estados anteriores se da por finalizado el procedimiento del monitoreo. Cabe recordar que este procedimiento se realiza en forma continua y repetitiva de acuerdo al periodo en que se considera necesario realizar el monitoreo de infraestructura.

Durante la interrupción o restitución de un incidente de infraestructura se realizará un análisis respectivo. Seguido se genera un informe con los tiempos de recuperación (tiempo medio entre fallos, paradas y entre incidentes), además se considerará realizar las recomendaciones respectivas y almacenar en una base de conocimiento para prevenir una interrupción del servicio a futuro.

A continuación se describen los términos utilizados anteriormente.

- **"Tiempo de detección:** tiempo desde el inicio de la falla hasta que se inicia la respuesta." (Osiatis, 2011).
- **"Tiempo de respuesta:** tiempo que transcurre desde la detección del hasta que se realiza un registro y diagnóstico del incidente." (Osiatis, 2011).
- **"Tiempo de reparación:** tiempo utilizado para reparar la falla o determinar una solución temporal a la misma y devolver el sistema a la situación anterior a la interrupción del servicio." (Osiatis, 2011).

Además se deben incluir en los informes de disponibilidad de los servicios los siguientes parámetros:

- **Tiempo Medio de Parada (Downtime):** tiempo promedio de duración de una interrupción de servicio, incluye el tiempo de detección, respuesta y resolución.
- **Tiempo Medio entre Fallos (Uptime):** tiempo medio durante el cual el servicio está disponible sin interrupciones.

- **Tiempo Medio entre Incidentes:** es el tiempo medio transcurrido entre incidentes que es igual a la suma del Tiempo Medio de Parada y el Tiempo Medio entre Fallos. (Osiatis, 2011).

Para la entrega de informes se propone considerar las recomendaciones necesarias al personal encargado de la infraestructura, teniendo en cuenta los porcentajes más altos de utilización de los recursos de hardware y software de los servidores monitoreados. Seguido se detallará los parámetros para el informe como respuesta a los tiempos medios entre parada, fallos e incidentes.

4.2.2.10. Informes de monitoreo.

En este punto se describe el formato de los informes de monitoreo que deben realizar los responsables de la Gestión de Disponibilidad y eventos mediante el apoyo de la herramienta de monitoreo HP SITESCOPE.

4.2.2.10.1. Formato de entrega del informe de monitoreo.

Los elementos principales a considerarse en el formato de entrega de informes de monitoreo que realizarán los responsables de la Gestión de Disponibilidad y eventos al monitoreo de infraestructura (servidores, red y base de datos) se describe en el anexo 4.

Se puede considerar una mejora al informe de monitoreo, esto dependerá de las consideraciones de la persona encargada del monitoreo de infraestructura de los servicios eSigef y eSipren.

4.2.2.11. Notificación de incidencias.

La idea es desarrollar un flujo detallado para las incidencias debido a la necesidad de considerar las respectivas notificaciones al personal sobre el impacto de cada incidente presentado.

Conforme vaya avanzado el tiempo de cada incidente, la notificación se realizará al administrador encargado de la infraestructura correspondiente.

La prioridad del incidente puede cambiar durante su ciclo de vida. Por ejemplo, se pueden encontrar soluciones temporales que restauren aceptablemente los niveles de

servicio y que permitan retrasar el cierre del incidente sin graves repercusiones.

Existen ocasiones en las que no se podrán resolver en primera instancia un incidente, para ello se deberá recurrir a un especialista que pueda tomar decisiones, a este proceso se le denomina **escalado**.

Los principales beneficios de una correcta monitorización y categorización de incidencias incluyen:

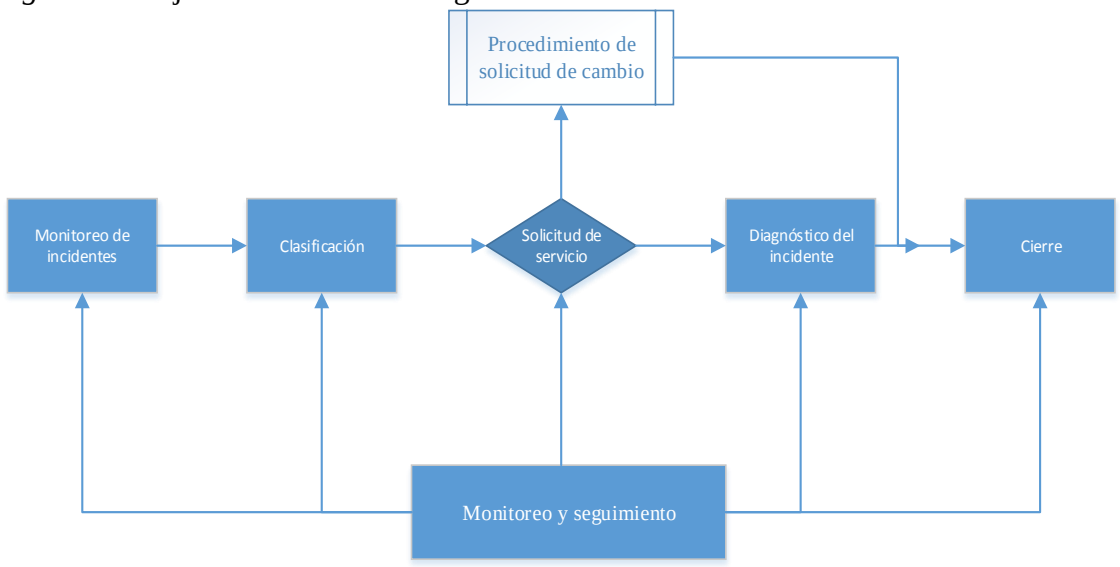
- Mejorar la productividad de los servidores.
- Mayor control en la monitorización de los servidores.
- Optimización de los recursos disponibles.
- Mejora de la satisfacción general de clientes y usuarios.

4.2.2.11.1. Flujo de la Gestión de Incidentes.

Es muy importante monitorizar los incidentes con el objetivo de recopilar toda la información que pueda ser utilizada para su resolución. El monitoreo y seguimiento de la gestión de incidentes está permanentemente ligado al flujo de las siguientes actividades:

- Monitoreo
- Clasificación
- Solicitud de servicio
- Procedimiento de solicitud de cambio
- Investigación y diagnóstico
- Cierre

Figura 32 Flujo de monitoreo de la gestión de incidentes

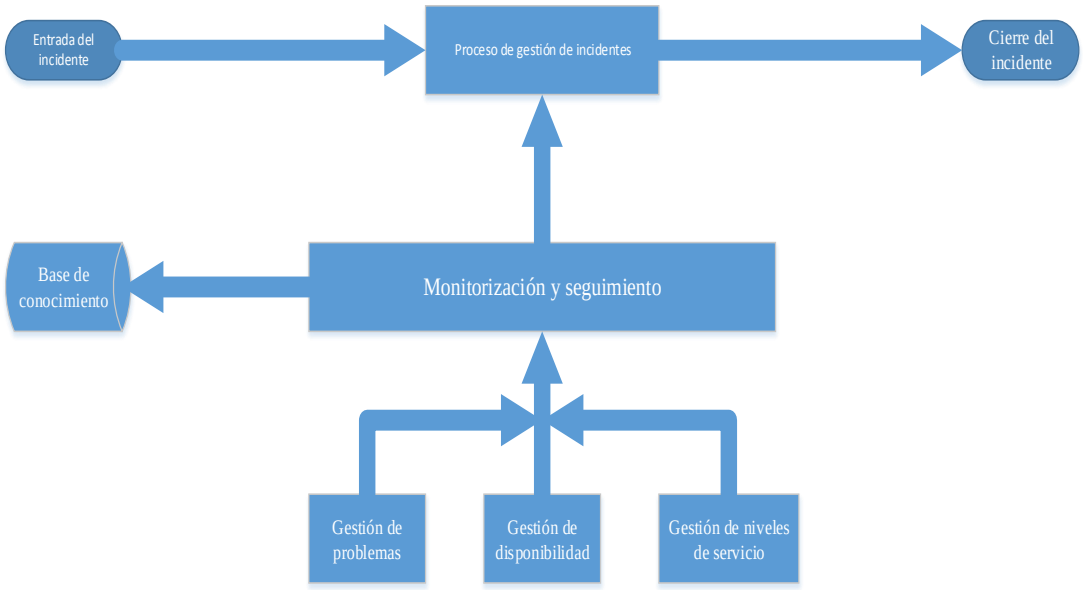


Fuente: (Osiatis, 2011)

4.2.2.11.2. Diagrama de los procesos implicados en la gestión de incidentes.

Dentro del proceso de la gestión de incidencias se encuentra algunos procesos que interfieren desde la entrada de un incidente hasta el cierre del mismo.

Figura 33 Los procesos implicados en la Gestión de Incidentes



Fuente: (Osiatis, 2011).

Los procesos más importantes a tomar en cuenta para el proceso de monitorización de las incidencias son:

- **Gestión de problemas:** Ayuda a la gestión de incidentes informando errores conocidos y posibles soluciones temporales.
- **Gestión de disponibilidad:** Utiliza información registrada sobre la duración, el impacto y el desarrollo temporal de los incidentes para elaborar informes sobre la disponibilidad real del sistema.
- **Gestión de niveles de servicio:** La gestión de incidentes debe tener acceso a los SLA acordados con el cliente para poder determinar el curso de las acciones a adoptar. La gestión de incidentes debe proporcionar informes sobre el cumplimiento de los SLA contratados.

4.2.2.11.3. Control del proceso.

En la evaluación del rendimiento de gestión de incidentes se debe realizar una correcta elaboración de informes.

Tabla 41

Control del proceso de Gestión de Incidentes

Informes	Descripción
Gestión de niveles de servicio	Cumplimiento de los SLAs (acuerdo nivel de servicio) y que se adopten medidas correctivas en un incidente incumplido.
Monitorizar la disponibilidad de infraestructura	Se establece con el propósito de conocer el grado de satisfacción del cliente por parte del servicio prestado de la primera línea de soporte y atención al cliente.
Identificar errores	Algunos protocolos que no se adecuen a la estructura de monitoreo hacia la infraestructura se les deberá tomar medidas correctivas.

Elaborado por: Wilman Sánchez

4.2.2.12. Notificación de problemas.

Es necesario tomar en cuenta los aspectos más relevantes en el monitoreo y notificación de la gestión de problemas como los que se exponen a continuación:

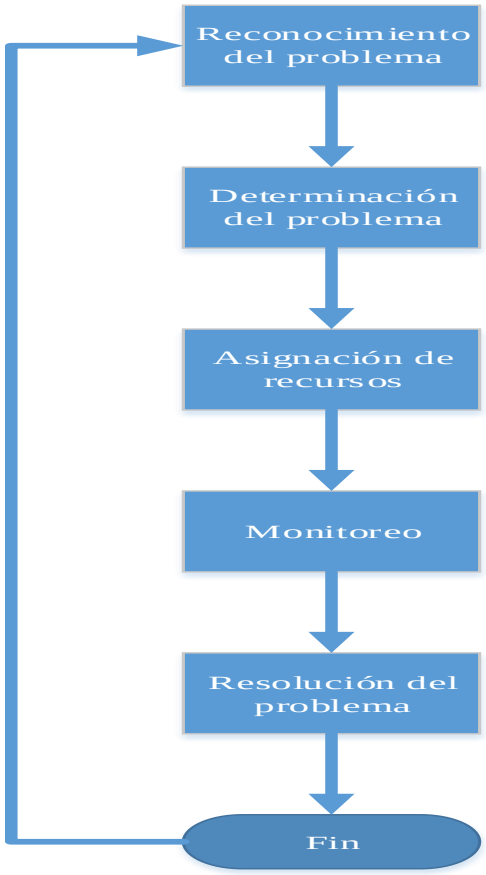
- **Reactiva:** Se analiza los problemas producidos con el objetivo de descubrir la posible causa y proponer las respectivas soluciones.
- **Proactiva:** Es necesario tener monitorizada toda la infraestructura TI a fin de prevenir posibles daños que afecten sustancialmente a los equipos que conforman los servicios más importantes de la empresa. También se deberá mantener

informada a toda la organización del comportamiento de los recursos de la infraestructura.

4.2.2.12.1 Flujo de la Gestión de Problemas.

En la figura 34 se presenta el flujo de actividades que se deben desarrollar en la gestión de problemas para garantizar la continuidad de los servicios eSigef y eSipren en el Ministerio de Finanzas.

Figura 34 Flujo de la Gestión de Problemas



Fuente: (Osiatis, 2011).

4.2.2.12.2. Procesos y actividades de la Gestión de Problemas.

La tabla 42 muestra los procesos y actividades que se deben desarrollar para una correcta gestión de problemas.

Tabla 42

Procesos y actividades de la Gestión de Problemas

Procesos	Actividades
Reconociendo el problema	Se identifica el evento o alerta y se captura la respectiva descripción.
Determinación del problema	Es necesario analizar, aislar, definir la solución del problema.
Asignación de recursos	La identificación y asignación de recursos es primordial seguido de una priorización de acciones con su respectiva notificación a usuarios, técnicos y coordinadores.
Monitoreo	Como parte primordial del esta actividad es necesario dar seguimiento al avance de la acción correctiva conjunto con el escalamiento del problema si así lo fuera necesario.
Resolución del problema	Completar y registrar las acciones correctivas para continuar con el cierre al incidente y notificar al usuario. De ser necesario se debe realizar un registro de la información para un análisis a futuro.

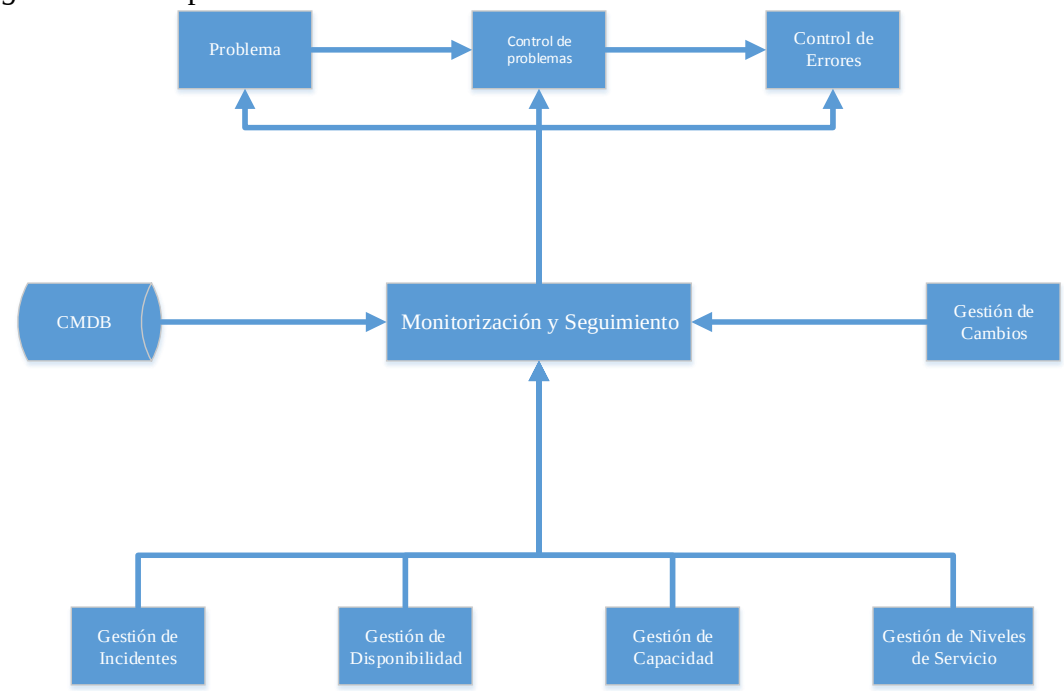
Elaborado por: Wilman Sánchez

4.2.2.12.3. Actividades de la Gestión de Problemas.

Entre las actividades más importantes relacionadas con la gestión de problemas se tienen las siguientes:

- **Control de problemas.-** Se registran y clasifican los problemas para determinar sus respectivas causas y convertirlos en errores conocidos.
- **Control de errores.-** Se registran los errores conocidos y se proponen dar soluciones a través de una solicitud de cambio que es remitida a la gestión de cambios.

Figura 35 Principales actividades de la Gestión de Problemas



Fuente: (Osiatis, 2011).

4.2.2.12.4. Control del proceso de la Gestión de Problemas.

Para una correcta gestión de problemas se debe elaborar los informes. A continuación se presentan dos principales consideraciones del control del proceso de la gestión de problemas.

Tabla 43

Control del proceso de la Gestión de Problemas

Informes	Descripción
Rendimiento de la gestión de problemas	Es necesario tener en cuenta el número de errores resueltos y la eficacia de las soluciones propuestas con tiempos de respuesta e impactos producidos.
Gestión proactiva	Se representan como acciones realizadas para la respectiva prevención de nuevos problemas. Además se considera necesario informar los resultados de los análisis realizados a la mejora de la infraestructura de la organización.

Fuente: (Desk, 2011).

4.2.2.13. Capacitación.

El personal responsable de la Gestión de Disponibilidad y eventos en el monitoreo, deberá capacitarse al menos cada 6 meses en temas relacionados con monitoreo de infraestructura. También debe asistir a talleres donde se establezcan charlas de casos de éxito en actividades relacionadas al monitoreo de infraestructura.

4.2.2.14. Aprobación de la propuesta.

Los aprobación de este propuesta de monitoreo apoyará a que las actividades a desarrollarse tengan un control y aseguren su buen desempeño. El Director Nacional de Operaciones y el Subsecretario Nacional de Innovación de las Finanzas Públicas decidirán sobre su implementación en la entidad del Estado.

CONCLUSIONES

- Luego de la revisión realizada a los procesos de ITIL V3 para el monitoreo de la infraestructura, se determinó los procesos de Gestión de Disponibilidad de Eventos son los que se adaptan al monitoreo de infraestructura y a la vez ayudan a incrementar la satisfacción de los administradores quienes son responsables de optimizar y monitorizar los servicios para que funcionen ininterrumpidamente y de manera fiable, cumpliendo los niveles de servicios establecidos, todo aquello a un costo razonable.

- La propuesta se realizó siguiendo las recomendaciones de los procesos de ITIL V 3, porque su metodología de trabajo ayudará a mantener la disponibilidad de los servicios eSigef y eSipren del Ministerio de Finanzas.

- Es importante considerar que en la generación de informes se debe detallar el tiempo medio entre fallos, paradas e incidentes. Debido a que esta información será de gran ayuda en la toma de decisiones de la alta gerencia en relación con los recursos de infraestructura y los servicios que están relacionados con la misma.

- Con la propuesta de monitoreo se ayudará a tomar decisiones en los equipos monitoreados, que permitan aprovechar al máximo la utilización del hardware, en las capas de presentación, aplicación y base de datos. De esta forma el cliente perciba una mayor calidad de servicio.

RECOMENDACIONES

- Implementar la propuesta del monitoreo de infraestructura que consta en el capítulo 4 para los servicios eSigef y eSipren en el Ministerio de Finanzas para lo cual se debe involucrar a la alta gerencia en seguimiento de las actividades a realizarse.

- Crear un área administrativa técnica para efectuar el monitoreo, supervisión y entrega de informes sobre la infraestructura.

- Adoptar las mejores prácticas de ITIL V3 en la Dirección Nacional de Operaciones, mediante capacitaciones a los analistas de infraestructura, para alcanzar un trabajo ordenado en el registro de incidentes y problemas ocurridos.

- Realizar charlas en la que se expongan las mejoras y los logros alcanzados con la implantación de este proyecto en otras áreas de tecnología, con la finalidad de continuar desarrollando un clima apropiado a futuro en proyectos similares.

LISTA DE REFERENCIAS

BCM. (2014). *www.bcm.com*. Recuperado el Lunes 23 de Diceimbre de 2013, de http://www.bmc.com/products/product-listing/ProactiveNet-Performance-Management.html

BMCsoftware. (2014). *Consola BMC*. Recuperado el Martes 26 de Noviembre de 2013, de http://documents.bmc.com/products/documents/37/83/83783/83783.pdf.

Bon, J. V. (2008, p. 28). *Fundamentos de la Gestión de Servicios de TI basada en ITIL*. Ediciones Van Haren Publishing, tercera edición.

Cloud, G. (2010). *GBM Cloud Services*. Recuperado el Miercoles 27 de Noviembre de 2013, de http://www.gbmcloud.com.

Deloitte. (2012). *deloitte.com.* Recuperado el Miercoles 18 de Diciembre de 2013, de www.deloite.com: http://www.deloitte.com

Desk, F. H. (2011). *Foros Help Desk*. Recuperado el Jueves 26 de Diciembre de 2013 de http://www.forohelpdesk.com/index.php?publicaciones_tips

Enterprices, N. (2009). *NAGIOS*. Recuperado el Jueves 12 de Diciembre de 2013, de http://www.nagios.org/

FMS, P. (2014). *pandorafms.com*. Recuperado el Lunes 09 de Diciembre de 2013, de http://pandorafms.com/Producto/pandora-servers/es

Hewlett-Packard. (2012). *hp.com.* Recuperado el Miercoles 27 de Noviembre de 2013, de http://www8.hp.com/us/en/software-solutions/software.html

HW-Group. (s.f.). *www.hw-group.com*. Recuperado el Miercoles 18 de Diciembre de 2013, de http://www.hw-group.com/software/pd_snmp_en.html#IBM_Tivoli

IBM. (2014). *ww.ibm.com*. Recuperado el Viernes 13 de Diciembre de 2013, de http://www.ibm.com/developerworks/ssa/downloads/tiv/tivolimonitoring/faq-ec2-tivolimonitoring.html

Informáticos, L. y. (s.f.). *lsi.us.* Recuperado el Jueves 12 de Diciembre de 2013, de http://www.lsi.us.es/: http://www.lsi.us.es/docencia/get.php?id=473

Lacoctelera. (2012). *lacoctelera.net*. Recuperado el Miercoles 25 de Diciembre de 2013, de so_prass.lacoctelera: http://so_prass.lacoctelera.net

LLC, T. (2013). *Seguridad Informática*. ecuperado el Miercoles 25 de Diciembre de 2013, de http://seguridadinformaticaufps.wikispaces.com/MAGERIT

Long, J. O. (2012, p. 5-24). ITIL 2011 At a Glance, Springer New Yoork. En J. O. Long, *IIL 2001 At a Glance* (págs. 5 - 24).

MHAP, M. d. (2012). Libro I - Método. En M. A. Gómez, *MAGERIT versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información* (pág. 7). Madrid: Ministerio de Hacienda y Administraciones Públicas.

Ministerio de Administraciones Públicas, M. (16 de junio de 2005). *epractice.* Recuperado el Miercoles 25 de Diciembre de 2013, de http://www.epractice.eu: http://www.epractice.eu/files/media/media_897.pdf

Ministerio de Finanzas. (2013). *Ministerio de Finanzas.* Recuperado el Lunes 06 de Enero de 2014, de www.finanzas.gob.ec.

Nagios. (2012). *Ventajas y desventajas*. Recuperado el Viernes 20 de Diciembre de 2013, de http://www.nagios-es.org/.

Nagios.org. (2012). *Ventajas e inconvenientes*. Recuperado el Lunes 23 de Diciembre de 2013, de http://www.nagios-es.org/.

Osiatis. (2011). *Osiatis ITIL V3.* Recuperado el Martes 12 de Noviembre de 2013, de www.osiatis.es.

protejete. (2012). *protejete*. Recuperado el Viernes 20 de Diciembre de 2013, de protejete.wordpress.com: http://protejete.wordpress.com/gdr_principal/amenazas_vulnerabilidades/

Sánchez, R. (s.f.). *www.slideshare.net*. Recuperado el Viernes 20 de Diciembre de 2013, de http://www.slideshare.net/Inteli_SC/midiendo-itil

scridb. (2011). *scribd.* Recuperado el Miercoles 20 de Noviembre de 2013, de http://es.scribd.com.

Soltero, J. (2004). *www.hyperic.com*. Recuperado el Viernes 20 de Diciembre de 2013, de http://www.hyperic.com/

STATUM. (20 de Febrero de 2014). *Nexo entre tecnología y negocio*. Recuperado el Viernes 20 de Diciembre de 2013, de http://www.statum.biz/web/guest;jsessionid

Tene, M. F. (Noviembre de 2012). *Universidad Técnica de ambato.* Recuperado el Viernes 20 de Diciembre de 2013, de http://repo.uta.edu.ec: http://repo.uta.edu.ec/bitstream/handle/123456789/2895/

Torres, L. A. (2013, p. 73). Plan de Seguridad de la Información. *Trabajo de Final de Máster*.

Wikipedia. (s.f.). *www.wikipedia.org*. Recuperado el Viernes 20 de Diciembre de 2013, de http://en.wikipedia.org/wiki/BMC_Software

zabbix. (2001 - 2014). *www.zabbix.com/*. Recuperado el Viernes 13 de Diciembre de 2013, de www.zabbix.com/es/

GLOSARIO

ITIL: La Biblioteca de Infraestructura de Tecnologías de Información

TI: Referente a tecnologías de información

SLA: Acuerdo de nivel de servicio.

TIC: Referente a tecnologías de información y comunicación.

CMDB: Base de datos de gestión de configuración.

SINFIP: Sistema Nacional de Finanzas Públicas.

CMDB: Base de Datos de la Administración de la Configuración.

LOGS: Registro de eventos durante un rango de tiempo en particular.

RAC: Opción software para el SGBD Oracle producida por la Corporación Oracle.

S.O.: Sistema Operativo.

FRAMEWORK: Conjunto estandarizado de conceptos, prácticas y criterios para enfocar un tipo de problemática particular que sirve como referencia, para enfrentar y resolver nuevos problemas de índole similar.

SGBD: Sistema de Gestión de Base de Datos.

IIS: Internet Information Services.

ASP.NET: Framework para aplicaciones web desarrollado y comercializado por Microsoft.

ESIGEF: Sistema de Administración Financiera del Sector Público.

ESIPREN: Sistema Presupuestario de Remuneraciones y Nómina.

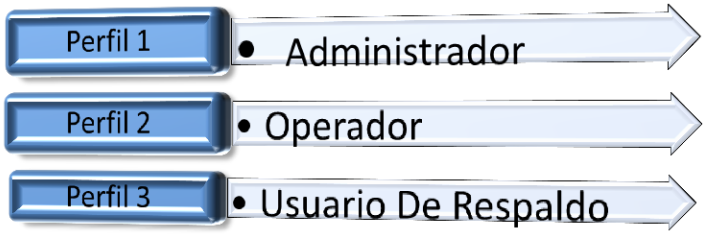
CI: Ítem de configuración.

ANEXOS

Anexo 1. Configuración de HP SITESCOPE

Para la configuración de la herramienta se comienza con el nivel de acceso de los perfiles que maneja cada servidor.

Figura 1 Perfiles de usuario

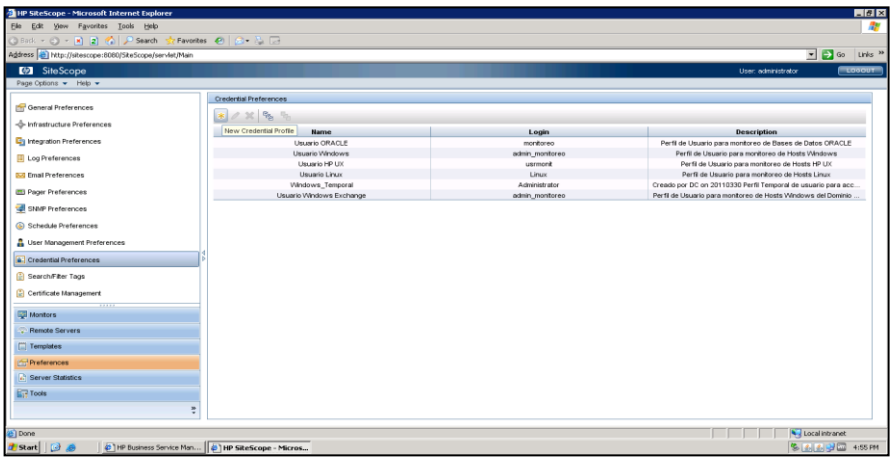


Fuente: (Hewlett-Packard, 2012)

Configuración de Perfiles

Para la configuración de perfiles se debe ingresar a la herramienta en el menú de preferencias (preferences) y luego en preferencia de credenciales (credential preferences), presionar el botón correspondiente a nuevo perfil de credenciales (new credential profile), como se muestra en la figura siguiente.

Figura 2 Perfiles de usuario

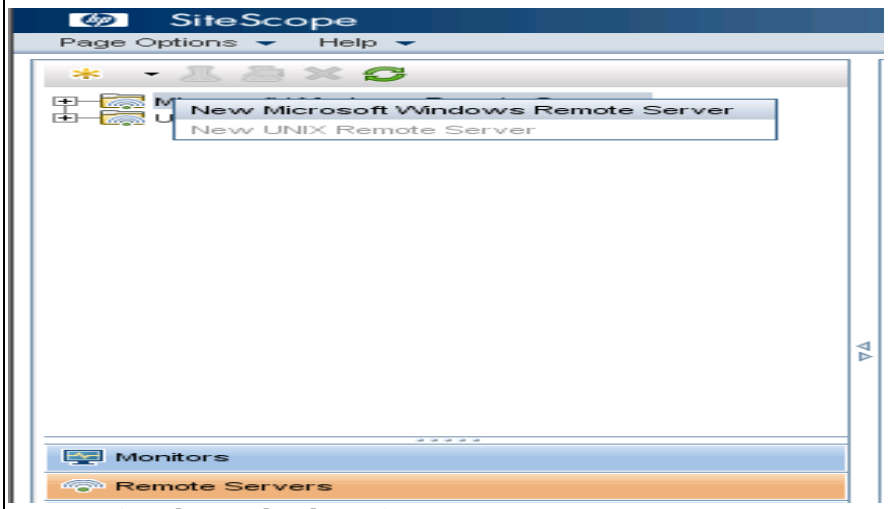


Fuente: **(Hewlett-Packard, 2012)**

Configuración de servidores remotos

Para la configuración de servidores remotos de Windows se debe ingresar a la herramienta por el menú de Servidores Remotos (Remote Servers) y luego hacer clic en Servidores Remotos Microsoft Windows (Microsoft Windows Remote Servers), presionar el botón Nuevo Servidor Remoto Microsoft Windows (New Microsoft Windows Remote Server), como se muestra en la siguiente figura:

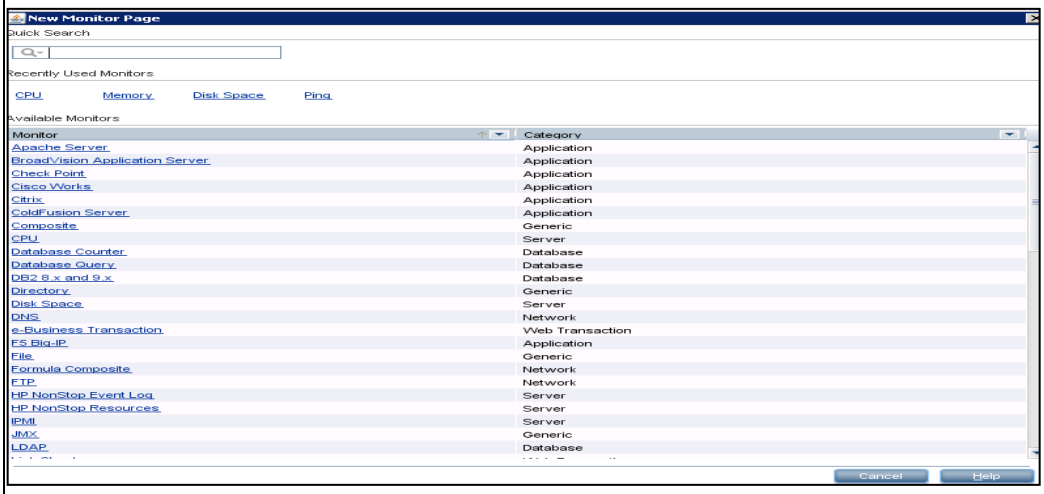
Figura 3 Servidores remotos



Fuente: **(Hewlett-Packard, 2012)**.

Configuración de la creación de monitores de disco: Ubicarse con el puntero del mouse sobre el grupo contenedor sobre el cual se va a crear el monitor, hacer clic derecho, sobre el menú emergente seleccionar la opción Nuevo > Monitor (New > Monitor). La página de nuevos monitores se despliega, se debe escoger de esta el monitor que se requiere crear.

Figura 4 Monitores de disco

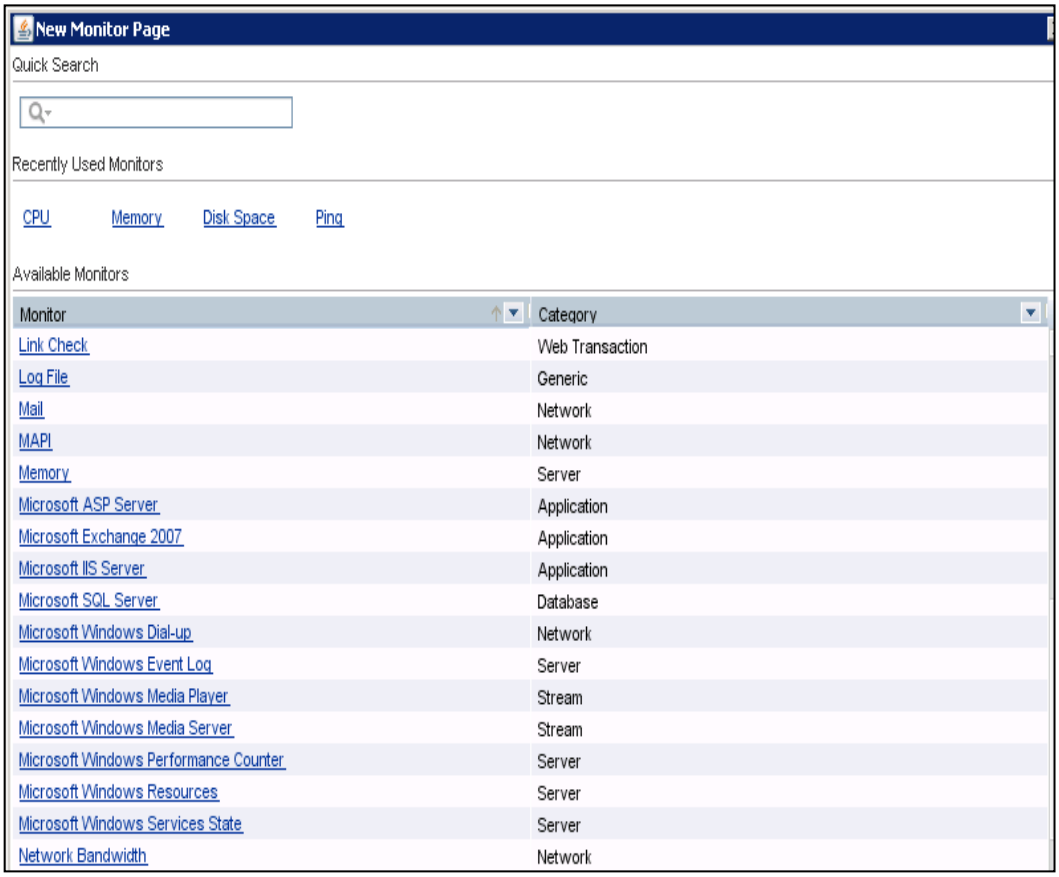


Fuente: (Hewlett-Packard, 2012)

Creación de los monitores de memoria: Ubicarse con el puntero del mouse sobre el grupo contenedor sobre el cual se va a crear el monitor, clic derecho, sobre el menú emergente seleccionar la opción Nuevo > Monitor (New > Monitor), esto como se muestra en la figura de creación de monitor de Disco.

La página de nuevos monitores se despliega, se debe escoger de esta, el monitor que se requiere crear.

Figura 5 Monitores de memoria

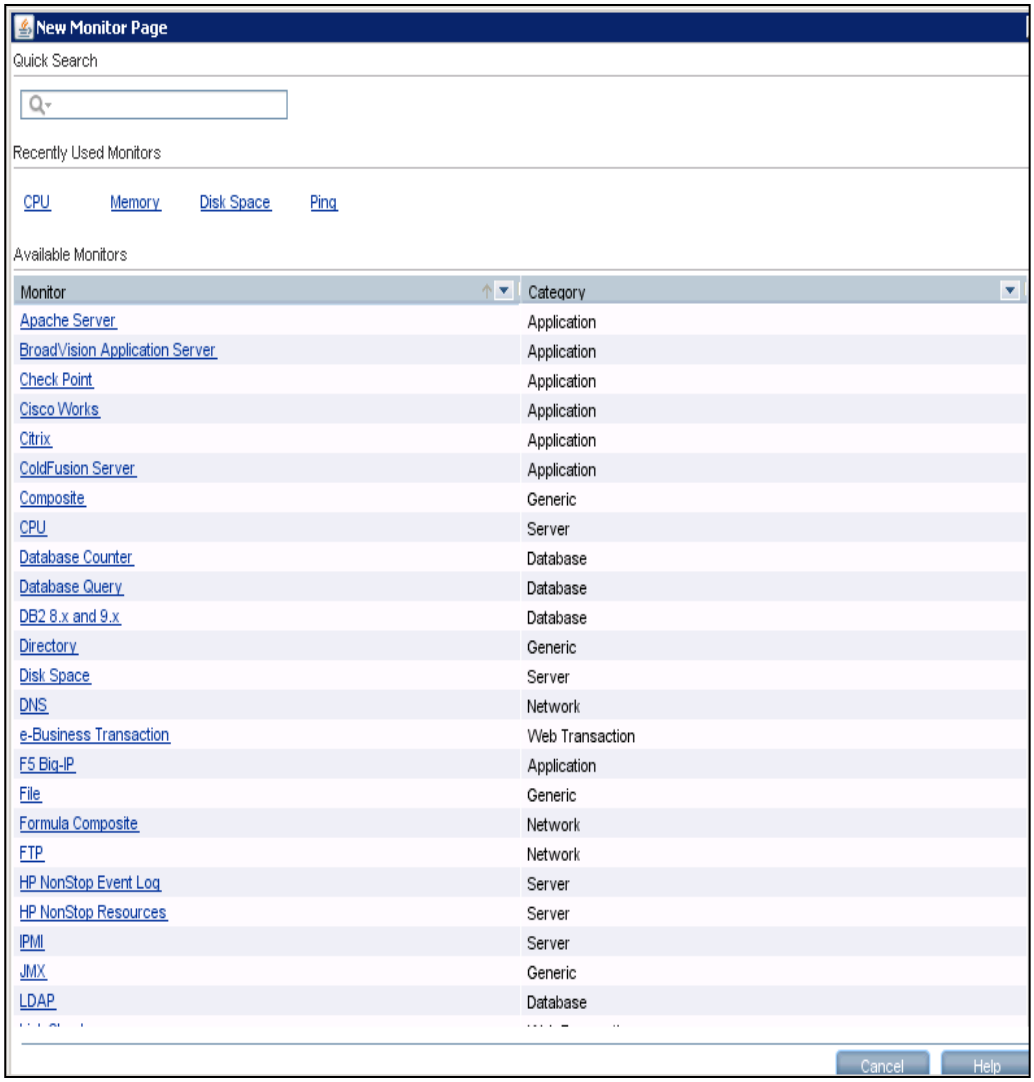


Fuente: (Hewlett-Packard, 2012)

Creación de los monitores para Procesador: Ubicarse con el puntero del mouse sobre el grupo contenedor sobre el cual se va a crear el monitor, clic derecho, sobre el menú emergente seleccionar la opción Nuevo > Monitor (New > Monitor), esto como se muestra en la figura de creación de monitor de Memoria.

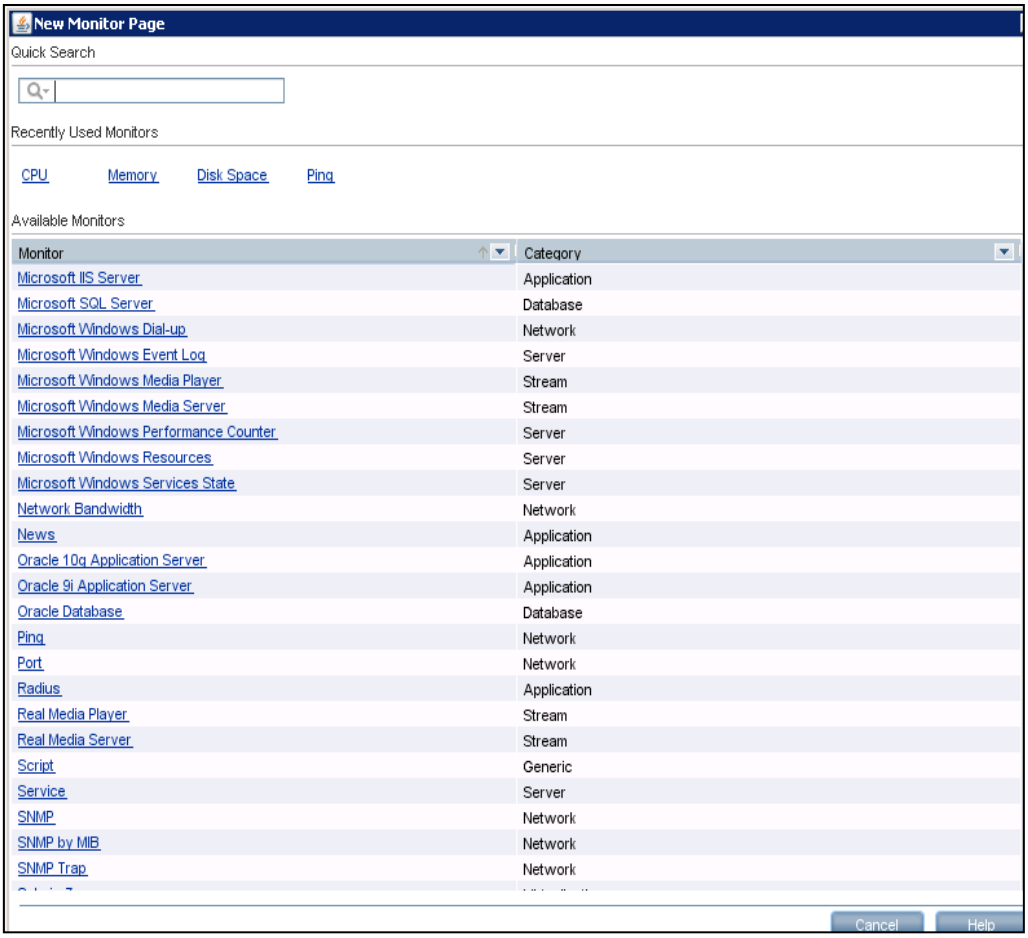
Creación de los monitores de servicios: Ubicarse con el puntero del mouse sobre el grupo contenedor sobre el cual se va a crear el monitor, clic derecho, sobre el menú emergente seleccionar la opción Nuevo > Monitor (New >Monitor), esto como se muestra en la figura de creación de monitor de Servicios.

Figura 6 Monitores para procesador



Fuente: (Hewlett-Packard, 2012).

Figura 7 Monitores de servicios



Fuente: **(Hewlett-Packard, 2012)**.

Anexo 2. Captura de monitoreo mediante HP SITESCOPE para Disponibilidad

Corresponde a la captura de información que se realizó desde el 3 hasta el 21 de febrero del 2014, durante los días laborables en el Ministerio de Finanzas, con el objetivo de relacionar a los procesos de Gestión de Disponibilidad y de eventos con la monitorización de la herramienta HP SITESCOPE. Para ello solamente se decidió recopilar información correspondiente a los 12 servidores de la granja de producción de los aplicativos eSigef y eSipren. Está captura pertenece a la disponibilidad y la generación de eventos que corresponde a cada uno de los indicadores mostrados en la tabla 17 del trabajo.

Captura de información mediante HP SITESCOPE - Disponibilidad																	
Indicador	**Servidor**	**Semana 1**					**Semana 2**					**Semana 3**					**Total**
		Día 1	**Día 2**	**Día 3**	**Día 4**	**Día 5**	**Día 1**	**Día 2**	**Día 3**	**Día 4**	**Día 5**	**Día 1**	**Día 2**	**Día 3**	**Día 4**	**Día 5**	
Disponibilidad de los servicios eSigef en relación al 99.99 % de disponibilidad establecida	ePRE01p	99.98%	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	**99.99%**
	ePRE02p	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	**99.99%**
	ePRE03p	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	**99.99%**
	ePRE60p	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	**99.99%**
	ePRE61p	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	**99.99%**
	eAPP01p	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	**99.99%**
	eAPP02p	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	**99.99%**
	eAPP03p	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	**99.99%**
	eAPP60p	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	**99.99%**
	eAPP61p	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	**99.99%**
	eBDD01p	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	**99.99%**
	eBDD02p	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%	**99.99%**

Captura de información mediante HP SITESCOPE - Disponibilidad																	
Indicador	**Servidor**	**Semana 1**					**Semana 2**					**Semana 3**					**Total**
		Día 1	**Día 2**	**Día 3**	**Día 4**	**Día 5**	**Día 1**	**Día 2**	**Día 3**	**Día 4**	**Día 5**	**Día 1**	**Día 2**	**Día 3**	**Día 4**	**Día 5**	
Número de caídas de los servidores de infraestructura de los servicios eSigef y eSipren	ePRE01p	1 caída	0 caídas	0 caídas	0 caídas	0 caídas	0 caídas	0 caídas	0 caídas	0 caídas	0 caídas	0 caídas	0 caídas	0 caídas	0 caídas	0 caídas	**1 caída**
	ePRE02p	0 caídas	0 caídas	0 caídas	0 caídas	0 caídas	0 caídas	0 caídas	0 caídas	0 caídas	1 caída	0 caídas	1 caída	0 caídas	0 caídas	0 caídas	**2 caídas**
	ePRE03p	0 caídas	0 caídas	0 caídas	0 caídas	0 caídas	0 caídas	0 caídas	0 caídas	0 caídas	0 caídas	0 caídas	0 caídas	0 caídas	1 caída	0 caídas	**1 caída**
	ePRE60p	0 caídas	0 caídas	0 caídas	0 caídas	0 caídas	0 caídas	0 caídas	0 caídas	0 caídas	0 caídas	0 caídas	0 caídas	0 caídas	0 caídas	0 caídas	**0 caídas**
	ePRE61p	0 caídas	0 caídas	0 caídas	0 caídas	0 caídas	0 caídas	0 caídas	0 caídas	0 caídas	0 caídas	0 caídas	0 caídas	0 caídas	0 caídas	1 caída	**1 caída**
	eAPP01p	1 caída	0 caídas	0 caídas	0 caídas	0 caídas	0 caídas	0 caídas	0 caídas	0 caídas	0 caídas	0 caídas	0 caídas	0 caídas	0 caídas	0 caídas	**1 caída**
	eAPP02p	0 caídas	0 caídas	0 caídas	0 caídas	1 caída	0 caídas	0 caídas	0 caídas	0 caídas	0 caídas	0 caídas	0 caídas	0 caídas	1 caída	0 caídas	**2 caídas**
	eAPP03p	0 caídas	0 caídas	0 caídas	0 caídas	0 caídas	0 caídas	0 caídas	0 caídas	0 caídas	0 caídas	0 caídas	0 caídas	0 caídas	0 caídas	0 caídas	**0 caídas**
	eAPP60p	0 caídas	0 caídas	0 caídas	0 caídas	0 caídas	0 caídas	0 caídas	0 caídas	0 caídas	0 caídas	1 caída	0 caídas	0 caídas	0 caídas	0 caídas	**1 caída**
	eAPP61p	0 caídas	0 caídas	0 caídas	0 caídas	0 caídas	0 caídas	0 caídas	0 caídas	0 caídas	0 caídas	0 caídas	0 caídas	0 caídas	0 caídas	0 caídas	**0 caídas**
	eBDD01p	0 caídas	0 caídas	0 caídas	0 caídas	1 caída	0 caídas	0 caídas	0 caídas	0 caídas	0 caídas	0 caídas	0 caídas	0 caídas	0 caídas	0 caídas	**1 caída**
	eBDD02p	0 caídas	0 caídas	0 caídas	0 caídas	1 caídas	0 caídas	0 caídas	0 caídas	0 caídas	1 caída	0 caídas	0 caídas	0 caídas	0 caídas	0 caídas	**2 caídas**
Duración media (average) de caídas del servicio eSigef	ePRE01p	5 min.	0 min	0 min	0 min	0 min	0 min	0 min	0 min	0 min	0 min	0 min	0 min	0 min	0 min	0 min	**5 min.**
	ePRE02p	0 min	0 min	0 min	0 min	0 min	0 min	0 min	0 min	0 min	5 min.	0 min	5 min.	0 min	0 min	0 min	**10 min.**
	ePRE03p	0 min	0 min	0 min	0 min	0 min	0 min	0 min	0 min	0 min	0 min	0 min	0 min	0 min	5 min.	0 min	**5 min.**
	ePRE60p	0 min	0 min	0 min	0 min	0 min	0 min	0 min	0 min	0 min	0 min	0 min	0 min	0 min	0 min	0 min	**0 min**
	ePRE61p	0 min	0 min	0 min	0 min	0 min	0 min	0 min	0 min	0 min	0 min	0 min	0 min	0 min	0 min	5 min.	**5 min.**
	eAPP01p	5 min.	0 min	0 min	0 min	0 min	0 min	0 min	0 min	0 min	0 min	0 min	0 min	0 min	0 min	0 min	**10 min.**
	eAPP02p	0 min	0 min	0 min	0 min	5 min.	0 min	0 min	0 min	0 min	0 min	0 min	0 min	0 min	5 min.	0 min	**10 min.**
	eAPP03p	0 min	0 min	0 min	0 min	0 min	0 min	0 min	0 min	0 min	0 min	0 min	0 min	0 min	0 min	0 min	**0 min**
	eAPP60p	0 min	0 min	0 min	0 min	0 min	0 min	0 min	0 min	0 min	0 min	5 min.	0 min	0 min	0 min	0 min	**5 min.**
	eAPP61p	0 min	0 min	0 min	0 min	0 min	0 min	0 min	0 min	0 min	0 min	0 min	0 min	0 min	0 min	0 min	**0 min**
	eBDD01p	0 min	0 min	0 min	0 min	5 min.	0 min	0 min	0 min	0 min	0 min	0 min	0 min	0 min	0 min	0 min	**5 min.**
	eBDD02p	0 min	0 min	0 min	0 min	5 min.	0 min	0 min	0 min	0 min	0 min	0 min	0 min	0 min	0 min	0 min	**5 min.**

Captura de información mediante HP SITESCOPE - Disponibilidad																	
Indicador	**Servidor**	**Semana 1**					**Semana 2**					**Semana 3**					**Total**
		Día 1	**Día 2**	**Día 3**	**Día 4**	**Día 5**	**Día 1**	**Día 2**	**Día 3**	**Día 4**	**Día 5**	**Día 1**	**Día 2**	**Día 3**	**Día 4**	**Día 5**	
Número de servicios y componentes sujetos a monitorización de disponibilidad	ePRE01p	Total: 14 componentes monitoreados para la infraestructura de los servicios eSigef y eSipren															
	ePRE02p																
	ePRE03p																
	ePRE60p																
	ePRE61p																
	eAPP01p																
	eAPP02p																
	eAPP03p																
	eAPP60p																
	eAPP61p																
	eBDD01p																
	eBDD02p																
Reportes de monitoreo de recursos (CPU, Memoria y Disco) de los servidores de eSigef y eSipren	ePRE01p	1 rep.	0 rep.	0 rep.	0 rep.	0 rep.	0 rep.	0 rep.	0 rep.	0 rep.	0 rep.	0 rep.	0 rep.	0 rep.	0 rep.	0 rep.	**1 rep.**
	ePRE02p	0 rep.	0 rep.	0 rep.	0 rep.	0 rep.	0 rep.	0 rep.	0 rep.	0 rep.	0 rep.	0 rep.	0 rep.	0 rep.	0 rep.	1 rep.	**1 rep.**
	ePRE03p	0 rep.	0 rep.	0 rep.	0 rep.	0 rep.	0 rep.	0 rep.	0 rep.	0 rep.	0 rep.	0 rep.	0 rep.	0 rep.	0 rep.	0 rep.	**0 rep.**
	ePRE60p	0 rep.	0 rep.	0 rep.	1 rep.	0 rep.	0 rep.	0 rep.	0 rep.	0 rep.	0 rep.	0 rep.	0 rep.	0 rep.	0 rep.	0 rep.	**1 rep.**
	ePRE61p	0 rep.	0 rep.	0 rep.	0 rep.	0 rep.	0 rep.	1 rep.	0 rep.	0 rep.	0 rep.	0 rep.	0 rep.	0 rep.	0 rep.	0 rep.	**1 rep.**
	eAPP01p	0 rep.	0 rep.	0 rep.	0 rep.	0 rep.	0 rep.	0 rep.	0 rep.	0 rep.	1 rep.	0 rep.	0 rep.	0 rep.	0 rep.	0 rep.	**1 rep.**
	eAPP02p	0 rep.	0 rep.	0 rep.	0 rep.	0 rep.	0 rep.	0 rep.	0 rep.	0 rep.	0 rep.	0 rep.	0 rep.	0 rep.	0 rep.	0 rep.	**0 rep.**
	eAPP03p	0 rep.	0 rep.	0 rep.	0 rep.	0 rep.	0 rep.	0 rep.	0 rep.	0 rep.	0 rep.	0 rep.	0 rep.	0 rep.	0 rep.	0 rep.	**0 rep.**
	eAPP60p	0 rep.	0 rep.	0 rep.	0 rep.	0 rep.	0 rep.	0 rep.	0 rep.	0 rep.	0 rep.	0 rep.	0 rep.	1 rep.	0 rep.	0 rep.	**1 rep.**
	eAPP61p	0 rep.	0 rep.	0 rep.	0 rep.	1 rep.	0 rep.	0 rep.	0 rep.	0 rep.	0 rep.	0 rep.	0 rep.	0 rep.	0 rep.	0 rep.	**1 rep.**
	eBDD01p	0 rep.	1 rep.	0 rep.	0 rep.	0 rep.	0 rep.	0 rep.	0 rep.	0 rep.	0 rep.	0 rep.	0 rep.	0 rep.	0 rep.	0 rep.	**1 rep.**
	eBDD02p	0 rep.	0 rep.	0 rep.	0 rep.	0 rep.	0 rep.	0 rep.	0 rep.	0 rep.	0 rep.	0 rep.	0 rep.	0 rep.	0 rep.	1 rep.	**1 rep.**

Captura de información mediante HP SITESCOPE - Eventos																	
Indicador	Servidor	Semana 1					Semana 2					Semana 3					Total - Eventos
		Día 1	Día 2	Día 3	Día 4	Día 5	Día 1	Día 2	Día 3	Día 4	Día 5	Día 1	Día 2	Día 3	Día 4	Día 5	
Número de eventos ocurridos por aplicativo e infraestructura monitoreada	ePRE01p	1 evento	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	1 evento
	ePRE02p	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	1 evento	0 eventos	0 eventos	1 evento	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	2 eventos
	ePRE03p	0 eventos	0 eventos	0 eventos	1 evento	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	1 evento
	ePRE60p	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos
	ePRE61p	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	1 evento	1 evento
	eAPP01p	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos
	eAPP02p	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	1 evento	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	1 evento	0 eventos	0 eventos	0 eventos	2 eventos
	eAPP03p	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos
	eAPP60p	0 eventos	0 eventos	1 evento	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	1 evento
	eAPP61p	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos
	eBDD01p	0 eventos	0 eventos	0 eventos	0 eventos	1 evento	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	1 evento	0 eventos	0 eventos	0 eventos	0 eventos	2 eventos
	eBDD02p	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos
Número de eventos ocurridos por CPU, Memoria y Disco	ePRE01p	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos
	ePRE02p	0 eventos	1 evento	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	1 evento	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	2 eventos
	ePRE03p	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	1 evento	0 eventos	0 eventos	1 evento
	ePRE60p	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos
	ePRE61p	0 eventos	0 eventos	0 eventos	0 eventos	1 evento	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	1 evento
	eAPP01p	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos
	eAPP02p	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	1 evento	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	1 evento
	eAPP03p	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos
	eAPP60p	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	1 evento	0 eventos	0 eventos	0 eventos	1 evento
	eAPP61p	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos

Captura de información mediante HP SITESCOPE - Eventos																	
Indicador	Servidor	Semana 1					Semana 2					Semana 3					Total - Eventos
		Día 1	Día 2	Día 3	Día 4	Día 5	Día 1	Día 2	Día 3	Día 4	Día 5	Día 1	Día 2	Día 3	Día 4	Día 5	
Número de eventos relacionados con el alto consumo del CPU y Memoria del eSigef y eSipren	ePRE01p	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos
	ePRE02p	1 evento	0 eventos	0 eventos	0 eventos	1 evento	0 eventos	0 eventos	0 eventos	1 evento	0 eventos	0 eventos	0 eventos	0 eventos	1 evento	0 eventos	4 eventos
	ePRE03p	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	1 evento	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	1 evento
	ePRE60p	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos
	ePRE61p	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	1 evento	0 eventos	0 eventos	0 eventos	0 eventos	1 evento
	eAPP01p	0 eventos	1 evento	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	1 evento	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	2 eventos
	eAPP02p	0 eventos	0 eventos	1 evento	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	1 evento	0 eventos	0 eventos	0 eventos	2 eventos
	eAPP03p	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos
	eAPP60p	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	1 evento	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	1 eventos
	eAPP61p	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	1 evento	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	1 eventos
Número de eventos de aplicación (.NET) e infraestructura para los servidores del eSigef y eSipren	ePRE01p	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	1 evento	0 eventos	0 eventos	0 eventos	1 evento
	ePRE02p	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos
	ePRE03p	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos
	ePRE60p	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	1 evento	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	1 evento
	ePRE61p	0 eventos	0 eventos	0 eventos	1 evento	0 eventos	0 eventos	1 evento	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	2 eventos
	eAPP01p	0 eventos	0 eventos	1 evento	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	1 evento	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	2 eventos
	eAPP02p	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	1 evento	0 eventos	1 evento
	eAPP03p	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	1 evento	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	1 evento
	eAPP60p	0 eventos	0 eventos	0 eventos	0 eventos	1 evento	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	1 evento	0 eventos	0 eventos	0 eventos	2 eventos
	eAPP61p	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos	0 eventos

Anexo 3. Umbrales en HP SITESCOPE

A continuación se detallan las principales plantillas con sus valores correspondientes a las mejores prácticas tomadas por HP para la configuración de umbrales en la herramienta de monitoreo SITESCOPE.

Tabla 1
SITESCOPE Microsoft IIS 6 Solution Template

Counter	Description	Warning	Error
Private Bytes	Shows the current number of bytes that this process has allocated that cannot be shared with other processes.	15000000	20000000
Working Set	Shows the current number of bytes in the working set of this process. The working set is the set of memory pages touched recently by the threads in the process. If free memory in the computer is above a certain threshold, pages are left in the working set of a process even if they are not in use. When free memory falls below a certain threshold, pages are trimmed from working sets. If they are needed, they are then soft-faulted back into the working set before they leave main memory.	15000000	20000000

Fuente: Hewlett-Packard

Tabla 2
IIS Server monitor

Counter	Description	Warning	Error
Bytes Transmitted/sec	Shows the rate at which the server is sending bytes on the network. This counter indicates how busy the server is.	64000	90000

Counter	Description	Warning	Error
Get Requests/sec	The rate, in seconds, at which HTTP requests that use the **GET** method have been made to the WWW service.	480	640
Bytes Total/sec	The sum of the rate, in seconds, at which data bytes have been sent and received by the WWW service.	48000	64000
Not Found Errors/sec	The rate, in seconds, at which requests were not satisfied by the server because the requested document was not found.	200	250
Current Connections	The number of active connections to the WWW service.	48	64
Files/sec	The rate, in seconds, at which files have been sent and received by the WWW service.	600	640

Fuente: Hewlett-Packard

Tabla 3
ASP.NET metrics

Counter Name in Dashboard	Metric Unit	Description
Application restarts	Number of items	Number of times the application has been restarted during the Web server's lifetime.
Applications running	Number of items	Number of currently running Web applications.
Request execution time	Milliseconds	The number of milliseconds that it took to execute the most recent request.
Request wait time	Milliseconds	The number of milliseconds the most recent request was waiting in the queue.
Requests current	Number of items	The current number of requests, including those that are queued, currently executing, or waiting to be written to the client. Under the ASP.NET process model, when this counter exceeds the requestQueueLimit defined in the processModel configuration section, ASP.NET begins rejecting requests.
Requests queued	Number of items	The number of requests waiting to be processed.
State server sessions active	Number of items	The current number of sessions currently active.
State server sessions total	Number of items	The total number of sessions.
Worker process restarts	Number of items	The number of times a worker process has restarted on the machine.
Worker process runnings	Number of items	The number of worker processes running on the machine.

Fuente: Hewlett-Packard

Tabla 4
CPU status metrics

Counter name in the dashboard	Metric unit	Description	Default Thresholds
utilization	% (Percent)	Average CPU utilization, in percentage (the average value among all CPUs present in the system)	Warning when >= 90% Error when 100%
utilization cpu #N	% (Percent)	CPU utilization for each CPU present in the system	Warning when >= 90% Error when 100%

Fuente: Hewlett-Packard

Tabla 5

Memory status metrics

Counter name in the dashboard	Metric unit	Description	Default Thresholds
percent used	% (Percent)	Total memory usage level	Error when > 90% Warning when > 80%
MB free	Megabytes	Total number of megabytes of virtual memory free	None
pages/sec	Units per second	Frequency of paging	None

Fuente: Hewlett-Packard

Tabla 6

Disk utilization metrics

Counter name in the dashboard	Metric unit	Description	Default Thresholds
Logical Disk\N\% Free Space	% (Percent)	Relative amount of the free space on each logical disk (for N="_Total", this is the average value)	Warning when <= 10% Error when <= 5%
Logical Disk\N\% Idle Time	% (Percent)	Relative amount of time when the disk is idle (for N="_Total", this is the average value)	None
Logical Disk\N\Disk read Bytes/sec	Units per second	Average number of bytes read every second from each logical disk (for N="_Total", this is the average value)	None
Logical Disk\N\Disk write Bytes/sec	Units per second	Average number of bytes written every second from each logical disk (for N="_Total", this is the average value)	None
Logical Disk\N\Free Megabytes	Megabytes	Number of megabytes free on each logical disk (for N="_Total", this is the average value)	None

Fuente: Hewlett-Packard

Tabla 7

Oracle Database Server Default Metrics - Tablespaces

Counter/Metric	Description	Default Threshold
Table space free extents	The number of tablespaces with room for less than two new extents.	Any values greater than 0 meaning that if any tablespace exists with room for less than two new extents, this metric will error.
Table space free space	This returns three values for any selected table space - free space in MB, total space in MB and free blocks.	
Undo header waits	The number of undo header waits.	
Undo segment total gets	Total undo segment gets.	
Undo segment total waits	Total undo segment waits.	
User calls	Number of times a user either logs on, parses a statement or executes a statement.	
User commits	Number of times users have committed their transactions.	
User rollbacks	Number of times users have rolled back changes that they have made.	

Fuente: Hewlett-Packard

Anexo 4. Descripción del informe de monitoreo a presentar

En el presente anexo se detalla el formato con el que se deberá presentar los informes de monitoreo, debido a que este factor se lo considera importante para la mantener la disponibilidad de los servicios eSigef y eSipren.

Tabla 8
Informe de monitoreo

Elementos del formato para presentación de informes de monitoreo	
Elementos	**Caracteristicas del elemento**
Portada	Se propone que contenga, el logotipo actualizado del Miniterio de Finanzas. Descripción del tipo de informe a considerar. La direccion a la que será entregado este informe. El autor de este informe.
Tabla de Contenido	Describir el contenido del documento a presentar.
Introducción del documento	Indicar cual es el proposito de la presentación de este docuemento.
Descripción del monitoreo de los Servidores	Se presenta una breve descripción del tipo de informe y el periodo en el que se lo realiza al servidor, seguido de una captura de pantalla y la presentación . Detallar las respectivas conclusiones a considerar.

Elaborado por : Wilman Sánchez

Anexo 5. Factibilidad del proyecto

Tabla 9

Costo del proyecto

Costo operativo	**Subtotal**
Derecho de trabajo de titulación	$200.00 (dólares)
Movilización/transporte	$100.00 (dólares)
Internet	$150.00 (dólares)
Total costos operativos	$**450.00** (dólares)
Materiales	**Subtotal**
Copias	$100.00 (dólares)
Impresora	$300.00 (dólares)
Cartuchos impresora	$200.00 (dólares)
Resmas de papel	$50.00 (dólares)
Total materiales	$**650.00** (dólares)
Gastos proyecto	**Subtotal**
Recursos Humanos	$500.00 (dólares)
Total gastos proyecto	$**500.00** (dólares)
Costos Totales	
Operativos	$**450.00** (dólares)
Materiales	$**650.00** (dólares)
Proyecto	$**500.00** (dólares)
Imprevisto 10 %	$**160.00** (dólares)
Costo Total del Proyecto	$**1760.00** (dólares)

Elaborado por: Wilman Sánchez